PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	5

Application Number	09/545,336
Filing Date	April 7, 2000
First Named Inventor	David M. Tumey
Art Unit	2623
Examiner Name	Craig Kronenthal
Attorney Docket Number	062916.004

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
- ☑ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation
- ☐ Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☑ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☑ Other Enclosure(s) (please Identify below):
  Acknowledgment Postcard

Remarks

Enclosed please find the original and 3 copies of Applicants' Appeal Brief for distribution to the panel members and Examiner.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Eric W. Cernyar		
Signature	Eric W. Cernyar		
Printed name	45,919		
Date	November 4, 2005	Reg. No.	45,919

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Eric W. Cernyar		
Typed or printed name	Eric Cernyar	Date	November 4, 2005

11-07-05

AF/2623
IFW

GUNN & LEE, P.C.

Tom D. Lee*
Michelle L. Evans
John C. Cave
Miguel Villarreal, Jr.
Eric W. Cernyar
Robert L. McRae
Robert A. McFall†

Of Counsel:
Kenneth A. Keeling‡
Sara K. Mooney Hinkley‡

Attorneys at Law
700 N. St. Mary's Street, Suite 1500
San Antonio, Texas 78205
Telephone: (210) 886-9500
Facsimile: (210) 886-9883

E-mail: ecernyar@gunn-lee.com
Web Site: www.gunn-lee.com

* Board Certified - Civil Trial Law
° Patent Agent Consultant
† Houston, Texas, Office (713) 680-1447
C. Donald Gunn (1936-1999)

062916.004

November 4, 2005

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RE: U.S. Patent Application Serial No. 09/545,336 filed April 7, 2000, entitled "Facial Image Verification Utilizing Smart-Card with Integrated Video Camera"

Dear Sir:

Enclosed please find the following items for filing on the above-referenced patent application:

1. Transmittal Form with Certificate of Transmission/Mailing;
2. 4 Copies of an Appeal Brief and "Claims and Evidence" Appendix;
3. Check in the amount of $250.00, representing the fee for filing an appeal brief; and
4. Acknowledgment Card.

I give the United States Patent and Trademark Office authorization to charge any under payment or over payments to Gunn & Lee, P.C. deposit account number 500808. Please stamp the enclosed acknowledgment card with the date of receipt and return it to my office for our records.

Sincerely,

Eric W. Cernyar

11/09/2005 CNGUYEN 00000042 09545336
01 FC:2402 250.00 OP

Enclosures
cc: Yevgeny Levitov (FaceKey) (w/encl.)

G:\TDL\FaceKey\09-545,336\Cover Ltr Appeal Brief.doc

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex Parte DAVID M. TUMEY

Appeal No. 2005-_____
Application No. 09/545,336
Filed: April 7, 2000
Group Art Unit: 2623
Examiner: Craig Kronenthal
Title: FACIAL IMAGE VERIFICATION UTILIZING SMART-CARD WITH INTEGRATED VIDEO CAMERA
Confirmation No.: 9586
Attorney Docket No.: 062916.004

APPELLANTS' BRIEF

Submitted by:

Eric W. Cernyar
Reg. No. 45,919
Gunn & Lee, P.C.
700 N. St. Mary's Suite 1500
San Antonio, Texas 78205
(210) 886-9500
(210) 886-9883 – FAX

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

I. REAL PARTY IN INTEREST

FaceKey Corporation is the assignee of the pending application and the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

Appellants, Appellants' legal representative, and FaceKey Corporation are not aware of any other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-14 are pending in this application. Claims 1, 2, and 3 are independent claims. Claims 4-14 depend directly or indirectly from claim 3. Each of claims 1-14 stand rejected. Applicants appeal the rejections of each of claims 1-14.

IV. STATUS OF AMENDMENTS

No amendment to the claims was filed subsequent to the final rejection dated June 15, 2005.

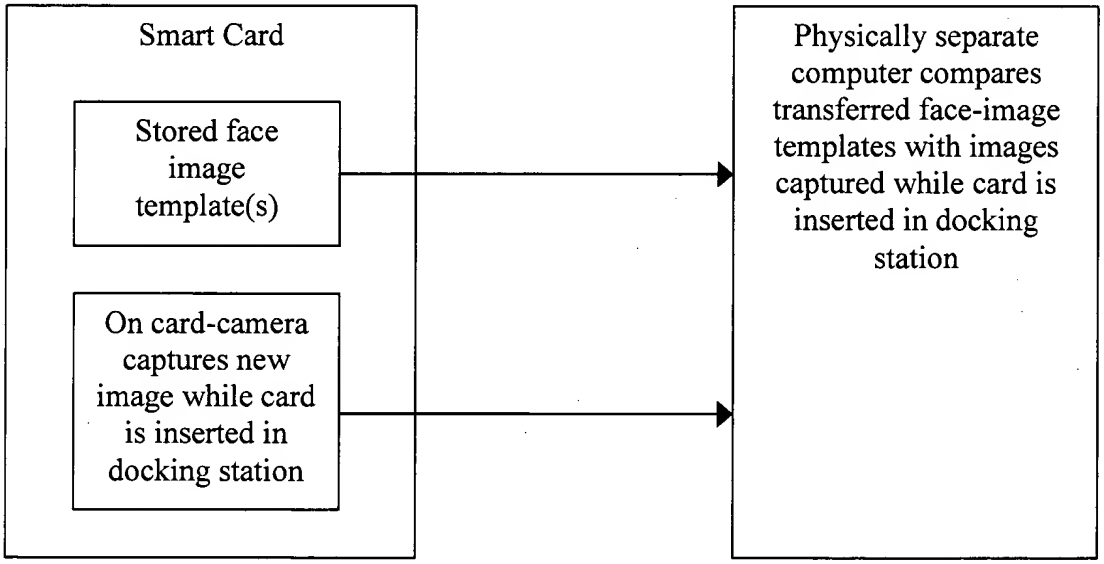
V. SUMMARY OF CLAIMED SUBJECT MATTER

Before specifically pointing out what each of the independent claims set forth, Appellants summarize the preferred embodiment taught by the specification. The pending patent application discloses a smart-card and facial-image based biometric verification system 10. The smart card 127 is equipped with a video camera 111, a digitizer 112, and internal non-volatile memory. The biometric verification system 10 also includes a smart card docking station 118 connected to a computer 113, which executes a face recognition software engine 130. *See* page 9, lines 2-18.

The smart card performs two main functions. First, it stores one or more biometric facial image templates associated with the smart card user. *See* page 6, lines 14-17; page 21, lines 3-

14. Second, when the smart card is inserted within the docking station at an access site, the video camera embedded within the smart card captures a new facial image from the user. Page 6, lines 7-10; page 10, lines 5-9; page 11, lines 9-13; page 21, lines 14-22. Both the biometric template and the fresh biometric information are then transmitted through the docking station 118 to the computer 113, which executes the face recognition software 130 to determine whether there is a match. Page 10, lines 7-13; page 21, lines 14-22.

As illustrated in the diagram below, the disclosed system 10 has three important characteristics: the biometric template is stored on the card (hereinafter referred to as "on-card biometric template"), access-site biometric capturing is done with the card (hereinafter referred to as "on-card biometric sensing"), and face recognition analysis is done off the card (hereinafter referred to as "off-card matching").



Claim 1 is generally directed to the facial image biometric verification system 10 described above. Claim 1 specifically claims a smart card 127 that is equipped with a video camera 111 to gather facial image data and a digitizer 112 for digitizing the facial image data. Claim 1 also claims a non-volatile memory to store the digitized facial image data, a smart-card

docking station 118 with a port for receiving the smart card 127 and communicating the digitized image data therethrough, and a communications interface 123 (*see also* communications cable 117) for transmitting the stored digitized facial image data from the docking station 118 to a central processor 116. *See* page 8, line 14 – page 11, line 5. Claim 1 also recites that the central processor 116, which is housed in a separate structure 113, runs the facial image verification routine 130. *Id.* Important characteristics of claim 1 include its structures for "on-card biometric template" storage, "on-card biometric sensing," and "off-card matching."

Claim 2 is directed to a method of facial image biometric verification, comprising an enrollment step in which facial image templates are created and stored on a smart card 127 equipped with a video camera 111, an access initiation step in which the smart card 127 is inserted into a docking port 118, and an image capture and verification step in which the smart card video camera captures fresh images and transmits those images to a central processor 116 that runs a facial image verification routine 130. Claim 2 also recites that the central processor 116 is housed in a separate structure 113. Important characteristics of claim 2 include the storage of an "on-card biometric template," and the functions of "on-card biometric sensing" and "off-card matching."

Claim 3, like claim 1, is also generally directed to a biometric verification system 10 like that described in the first paragraph of this section. Claim 3, however, is not limited to biometric facial images. Claim 3 recites "a portable identification device" (e.g., a smart card 127) that stores "a prerecorded representation of biometric data identifying an individual" (e.g., a biometric template), a "sensor configured to capture biometric data" (e.g., a video camera 111), and a communications interface that transmits both the prerecorded representation of biometric data, and the biometric data captured by the sensor. Claim 3 also recites a "communications

port" 118 that is external to the personal identification device 127 and which is adapted to receive information from the personal identification device 127. Finally, claim 3 recites a separately housed "processor" 116 communicatively coupled to the communications port 118 and configured to run a biometric verification routine 130 on the template and fresh biometric information received from the portable identification device 127. Important characteristics of claim 3 include its structures for "on-card biometric template" storage, "on-card biometric sensing," and "off-card matching."

Claim 10, which depends from claim 3, further recites that there are multiple biometric templates (i.e., multiple facial images) of the same individual stored on the "portable personal identification device" 127.

Claim 11, which depends from claim 3, further recites that different types of biometric template information (e.g., fingerprint *and* facial images) are stored on the "portable personal identification device." 127.

Claim 12, which depends from claims 10 and 3, further recites that the personal identification device is configured to automatically remove underutilized prerecorded representations of facial images.

Claim 13, which depends from claims 5, 4, and 3, further recites that the docking station and sensor on the smart card are positioned to facilitate a good quality facial image capture of a user during routine insertions of the smart card into the docking station.

Claim 14, which depends from claim 3, further recites that the sensor is an image-capturing device operable to capture at least two facial images of the individual, and wherein the processor is configured to compare the two facial images to detect motion.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner rejected claims 1-11 under 35 U.S.C. § 103(a) as being unpatentable over Burger (USPN 6,219,439) (**Exhibit C**) in view of Morinaga (USPN 6,137,685) (**Exhibit D**).

The Examiner rejected claim 12 under 35 U.S.C. § 103(a) as being unpatentable over Burger in view of Morinaga and further in view of Pare, Jr. (USPN 5,802,199) (**Exhibit E**).

The Examiner rejected claim 13 under 35 U.S.C. § 103(a) as being unpatentable over Burger in view of Morinaga and in further view of Tal (USPN 4,975,969) (**Exhibit F**).

The Examiner rejected claim 14 under 35 U.S.C. § 103(a) as being unpatentable over Burger in view of Morinaga and in further view of Turk et al. (USPN 5,164,992) (**Exhibit G**).

VII. PROCEDURAL HISTORY

This application has had a long history. A non-provisional application with two independent claims was filed on April 7, 2000, claiming priority to the non-provisional that was filed on April 9, 1999.

On December 19, 2000, the Examiner issued a first office action rejecting those claims under 35 U.S.C. § 103(a) over U.S. Patent No. 6,038,333 to Wang in view of U.S. Patent No. 5,180,901 to Hiramatsu and U.S. Patent No. 6,137,685 to Morinaga. Applicants traversed the rejections.

In the second office action, dated September 19, 2003, the Examiner withdrew those rejections but re-rejected the claims, this time over Morinaga in view of Wang. Applicants traversed the rejections again, and added claims 3-11.

On February 24, 2004, the Examiner issued a third and final office action again rejecting claims 1-2 over Morinaga in view of Wang, and rejecting claims 3-11 in view of U.S. Patent No. 5,623,552 to Lane. Applicants traversed these rejections again.

On May 12, 2004, the Examiner issued an advisory action re-affirming the rejections. On June 24, 2004, Applicants filed a RCE, a 37 CFR 1.132 Affidavit, and amendments to claims 1-3.

On October 4, 2004, the Examiner issued a fifth office action agreeing that the amendments rendered the previous rejections moot. But the Examiner rejected the claims over new art, particularly, over Burger in view of Morinaga and the other references. On October 4, 2004, Applicants traversed the rejections.

On June 15, 2004, the Examiner renewed these rejections in its sixth, and once again final, office action. This appeal proceeds from this sixth office action.

VIII. SUMMARY OF ARGUMENT

Claims 1-14 are patentable over Burger in view of Morinaga and the other cited references, because the references provide no motivation to combine certain selected elements from Morinaga and Burger together, and discard other ones, *in the specific manner claimed.* Claims 1-14 are also patentable over Burger in view of Morinaga and the other cited references because Burger expressly teaches – and *away* from the claimed invention[1] – that the biometric scanner element and verification circuitry should be kept in a "self-contained" unit. Claims 1-14 are also patentable over Burger in view of Morinaga and the other cited references in light of the Applicants' section 1.132 evidence[2] (attached in the Evidence Appendix as **Exhibit B**), which shows that the claimed invention occupies a niche between conventional smart-card systems and match-on-card systems. The 1.132 evidence further shows that both old and contemporary

[1] As noted in the "Summary of the Claimed Invention" section above, all of the claims require "on-card biometric sensing" and "off-card matching."

[2] This evidence was submitted with the Applicants' Request for Continued Examination on June 24, 2004. The Examiner formally acknowledged and presumably thereby entered the evidence into the record in the June 15, 2005, Final Office Action, at ¶ 2

references on match-on-card systems (including the closest prior art references) teach away from the claimed invention.

IX. ARGUMENT

A. Claims 1-11 are patentable over Burger in view of Morinaga because there is no persuasive evidence of any teaching, suggestion, or motivation to combine certain selected elements from Morinaga and Burger together, and discard other ones, in the specific manner claimed – and in a manner which goes against the teachings of Burger and other prior art references.

1. Overview of The Burger Reference

The Burger reference describes a smart card system comprising a smart card 14 and a smart card reader 12. The smart card 14 holds a fingerprint template in memory 20. The smart card reader 12 (*not the smart card 14 itself*) is equipped with a fingerprint scanner 16. The smart card reader 12 also includes a comparison chip 19 to compare the fingerprint template with a freshly-acquired fingerprint scan.

FIG. 1

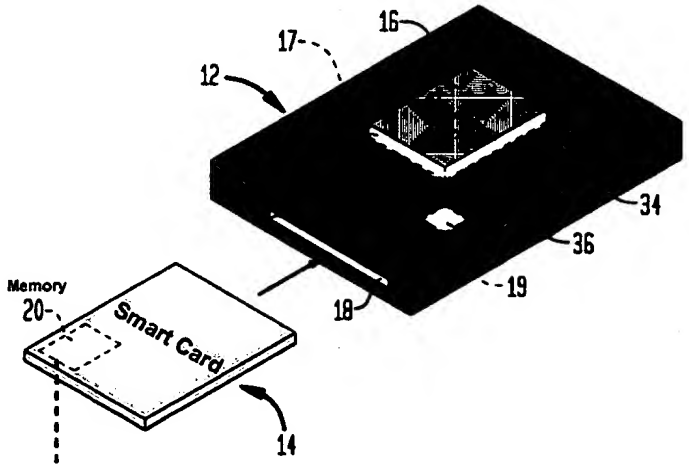
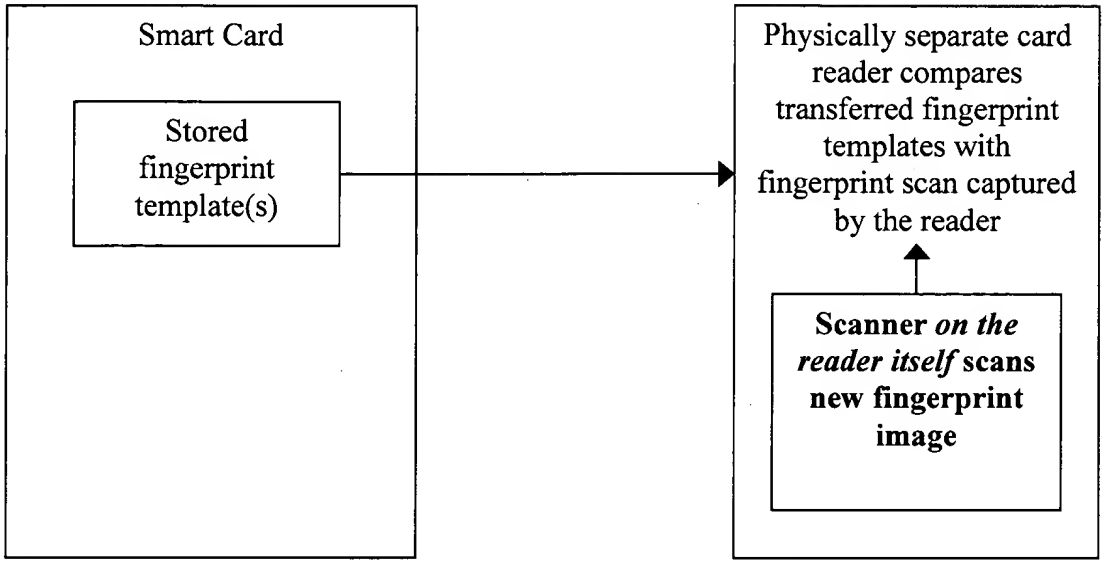


Figure 1 from Burger
(coloring and labeling added)

Burger's biometric verification architecture[3] is illustrated in the diagram below (which contrasts with the diagram illustrated on page 2 of this brief):



2. *Overview of The Morinaga Reference*

The Morinaga reference is not at all concerned with, and has no relation to the field of, biometric recognition. Morinaga is directed to a "portable electronic information device for performing information processing, data communication or the like" (see Abstract) comprising (1) a portable "device body 1" with structure to perform "information processing, data communication, or the like" (col. 1, lines 15-17), and (2) "a card-shaped information medium 4 called an IC (integrated circuit) card having a memory function or the like" (col. 1, lines 19-21) that can be inserted into the device body. The portable electronic information device body 1 may

---

[3] According to Burger's Abstract and the Background section to the specification, the principle advantage of this architecture is that at least a "first level authentication" (col. 2, lines 40-57) is done on the reader itself before any information is communicated to a server, thereby preventing user data from being stolen or sniffed out:

> The system is self-contained so that the comparison of the biometric data with the data stored on the chip is done immediately on board the reader without relying upon communications to or from an external source in order to authenticate the user. The invention also prevents communication with external sources prior to user authentication being confirmed, so as to prevent user data from being stolen or corrupted.

use "the memory or the like of the card-shaped information medium 4" to perform information processing. Col. 1, lines 19-27. According to Morinaga, a problem with the prior art was that the bodies of *conventional* portable electronic information devices (tablet computers or PDAs, perhaps?)[4] for receiving the card was too bulky. Col. 1, lines 30-45. Therefore, Morinaga proposes a space-saving physical interface on the card-reading device for receiving the card.

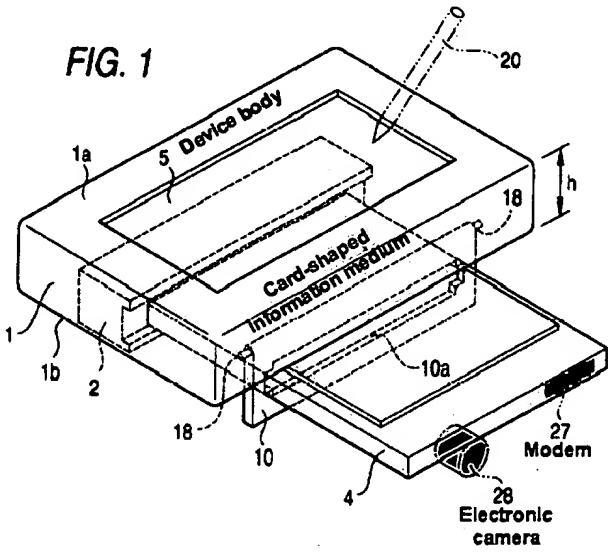


Figure 1 from Morinaga
(coloring and labeling added)

Most of Morinaga's disclosure is concerned with the physical interconnection between the slot and the card. Morinaga is extremely general about the functionality of the card. Basically, Morinaga suggests that the card could embody anything – a memory card, a modem card, or a camera card.

Morinaga has only 2 sentences describing the camera card embodiment (which follow two other sentences describing the modem card embodiment), namely:

---

[4] Morinaga says that the "portable electronic information device" was "a conventional device" (col. 1, line 31), but he does not get anymore specific than that. Furthermore, easily-accessible sources do not suggest what Morinaga had in mind. (A search of assignee Funai Electric's website indicates that the company makes large-screen plasma HDTV display panels, DVD recorders, and LCD televisions – which are not typically small and portable.) Given Morinaga's goal of making the device body "small in size so as not to be bulky at the time of carrying it" (col. 1, lines 50-52), perhaps *conventional* "portable electronic information devices" included tablet computers and PDAs.

> Further, as shown in FIG. 1, an electronic camera 28 may be provided at the card-shaped information medium 4. In such an arrangement, an image can be photographed by using the electronic camera 28, and an address table with face pictures can be prepared easily by combining the photographed images and an address table.

Morinaga suggests only a single function be performed with the images – that they be combined with an "address table."[5] Morinaga does not suggest that the images be used with an image recognition system, as claimed in claims 1 and 2. Morinaga also does not indicate where on this "arrangement" – the camera card 4 or the device body 1 – the "address table with face pictures" is to be prepared.[6] Morinaga does not even indicate whether this *camera card embodiment* includes non-volatile memory – it is quite possible that Morinaga contemplated direct transfer of the images from the camera card 4's digital imaging circuitry to memory on-board the device body 1. Morinaga simply says too little to know one way or the other.

3. The Examiner's Arguments

In the Final Office Action, the Examiner acknowledged that Burger "does not disclose that a silicon-based video camera is embedded within said smart card for gathering facial image data or a digitizer integrated within said smart card for digitizing said facial data." *Final Office Action*, at 5. But, the Examiner argues, "[i]t would have been obvious to one of ordinary skill in the art at the time the invention was made to embed a video camera (in place of Burger's fingerprint sensor 16 provided on the reader 12) within said smart card for gathering facial image data as taught by Morinaga and including a digitizer for digitizing said facial image data in order

---

[5] It is not clear what kind of "address table" Morinaga has in mind. It could be a table that lists contact information, including the photographed subjects' residential addresses. It could instead refer to electronic addresses – i.e., pointers to locations in computer memory. There is simply too little context to tell what was meant.

[6] For that matter, Morinaga does not suggest how his "arrangement" makes the preparation of an address tables with face pictures any "easier" than other arrangements. Indeed, it does not appear that generating address tables with face pictures is even remotely relevant to Morinaga's invention – which was to provide a space-saving physical interface between the device body 1 and the card 4.

to photograph facial images and prepare an address table of photographed facial images, for example, to recognize a human user similar to Burger's authentication using fingerprints." *Id.*

As evidence of some motivation, teaching, or suggestion to combine the references, the Examiner argued that Morinaga's very mention of "face pictures" "suggests that [Moringa's] card would be used in a biometric identification system," that Morinaga's small size would make it suitable for use as an ID-based smart card, and that Burger itself (at col. 4, lines 31-33) suggested that other forms of biometric identification could replace the fingerprint scanner. *Final Office Action*, at 3.

4. There is no prima facie basis for combining Burger with Morinaga in the manner claimed (applicable to all claims)

The Examiner's obviousness rejection should be reversed because it (1) overstates what Morinaga discloses and suggests; (2) fails to explain why skilled artisans would combine certain selected elements from Morinaga and Burger together, and discard other ones, *in the specific manner claimed*; (3) ignores Burger's teachings away from the specifically-claimed combination; and (4) also gives no consideration to the Applicants' section 1.131 evidence.[7]

In *Graham v. John Deere Co.*, the Supreme Court cautioned officials "to resist the temptation to read into the prior art the teachings of the invention at issue."[8] But the Examiner succumbed to that temptation by reading a teaching or suggestion of biometric identification into Morinaga's mention of combining photographic "face pictures" with an address table. There are many potential uses for a database of face pictures, other than biometric verification. For example, one might wish to store pictures along with their other "contact" information on their personal digital assistant (PDA).

---

[7] This fourth factor will be discussed in part 5, below.

[8] *Graham v. John Deere Co.*, 383 U.S. 1, 36, 148 U.S.P.Q. 459 (1966).

Unless one reads a suggestion of biometric applications from the invention at issue *into* the Morinaga reference, there is simply no motivation, suggestion or teaching for combining anything other than – perhaps – the space-saving features of Morinaga's *device body* with Burger's smart card reader.[9] Neither reference provides any motivation for replacing Burger's biometric scanner on a smart card reader with a biometric scanner on the smart card itself. The mere fact that Burger *can* be combined or modified in this way does not render the resultant combination or modification obvious.[10]

To sustain an obviousness rejection, an examiner "must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed."[11] Burger teaches putting the fingerprint reader 16 (or, alternatively, structure for performing some other kind of biometric scan – *see* col. 4, lines 31-33), on the smart card reader 12 itself, together with the comparison chip 19 used to perform the biometric comparison. The Examiner can argue that a person of ordinary skill in the art might modify the Burger smart card reader to incorporate the space-saving features of Morinaga. But the Examiner would presumably not cite any motivation to modify the Burger smart card to include Morinaga's *modem* (see col. 5, lines 34-37). Likewise, there is no reason, evident from the cited references, that a skilled artisan would replace Burger's on-reader fingerprint reader 16 with Morinaga's on-

---

[9] Burger does teach that one of its features is that it is "self-contained, portable," and can be "hand-held." *See* col. 4, lines 3-37). Morinaga is directed to an interconnection that enables one to make the body of "a portable electronic information processing device" "small in size so as not to be bulky at the time of carrying it." *See* col. 1, lines 50-52. This would, at most, provide motivation to appropriate the space-saving features of Morinaga's device body into Burger – but this would not provide any motivation to modify Burger's *smart card* itself. After all, Morinaga does not describe any structural modifications intended to reduce the size of the smart card itself.

[10] *In re Mills*, 916 F.2d 680, 682, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990); *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) ("The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification.").

[11] *In re Rouffet*, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453 (Fed. Cir. 1998) (emphasis added).

card video camera 28. There is simply no reason that a skilled artisan would combine Burger and Morinaga *in the manner claimed.*

It is important to keep in mind the different contexts to which the Morinaga and Burger references were directed, before combining them to make an obviousness rejection. In "determining whether an inventor would reasonably be motivated to go to the field in which the examiner found the reference, in order to solve the problem confronting the inventor, . . . it is necessary to consider '*the reality of the circumstances*' – in other words, *common sense* – in deciding in deciding in which fields a person of ordinary skill would reasonably be expected to look for a solution to the problem facing the inventor."[12] Morinaga was directed to "conventional" portable electronic information devices. Col. 1, line 31. PDAs and portable computers are conventional portable electronic information devices. At the time of the Morinaga invention (1997), relatively few (if any) portable PDAs included built-in cameras – but it was possible to extend the functionality of a PDA or portable computer by adding a modem or camera card – which may be why Morinaga briefly mentioned the possibility in his patent.

Image of (modern) Casio CompactFlash Digital PDA Camera Attachment

But Burger's smart card reader already incorporated structure for biometric scanning. So it is difficult to rationalize why an artisan would turn to Morinaga's teachings regarding a camera card to replace Burger's on-the-card-reader biometric scanner with a smart-card-mounted biometric scanner. It would be as if someone with a PDA that *already has* an integrated camera

[12] *In re Oetiker*, 977 F.2d 1443, 1447, 24 U.S.P.Q.2d 1443 (Fed. Cir. 1992) (emphasis added).

bought a camera card. In sum, Morinaga's teachings about a camera card should not be taken out of context, but instead "must be considered in the context of the teaching of the entire reference."[13]

The Examiner's rejection also picks and chooses certain of Morinaga's teachings – while disregarding others – in order to support the rejection. For example, the Examiner, in a previous rejection involving Morinaga and a different reference, argued that "it is obvious if not inherent that the images are stored and/or processed on the [Morinaga's] card itself." Office Action dated Feb. 24, 2004, at ¶ 3. But in the *latest* rejection, the Examiner ignores Morinaga's teaching to perform the "information processing" (which could include biometric comparisons) on the smart card 14 itself – as Morinaga suggests on col. 1, lines 24-27 – because such a combination would *not* read on the claims (which require off-card matching). "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art."[14]

The Examiner's rejection also ignores Burger's own teachings, by modifying Burger in a manner that contradicts one of the stated objects of Burger's invention. The Examiner's combination isolates the biometric scanning (by moving it from the reader, where Burger had it, to the card, as claimed) from the biometric verification (keeping it off the card and on the reader, as Burger teaches). But two of Burger's principal objects are to provide an authentication system which is both "self-contained" and "which prevents 'hacking' or other unauthorized access to the authentication process and data." Col. 3, lines 61-67. Burger accomplishes these purposes by keeping the biometric-scanning hardware and biometric verification circuitry in a single, "self-

[13] *In re Kotzab*, 217 F.3d 1365, 1371, 55 U.S.P.Q.2d 1313 (Fed. Cir. 2000).

[14] *In re Hedges*, 783 F.2d 1038, 1041, 228 U.S.P.Q. 685 (Fed. Cir. 1986).

contained" unit: "The comparison of the fingerprint scanned at the scanner 16 with the data on the chip 20 of the smart card 14 is done immediately on board the reader 12." Col. 5, line 66 – col. 6, line 1. In this manner, Burger prevents unauthorized access to authentication data, including the actual fingerprint scan.

"A prima facie case of obviousness can be rebutted if the applicant ... can show 'that the art in any material respect taught away' from the claimed invention."[15] "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, ... would be led in a direction divergent from the path that was taken by the applicant."[16] Burger's teachings led in a direction divergent from the Examiner's combination, which exposes not only the stored biometric template, but also the freshly scanned biometric information, to interception by a hacker. Although there may be other ways (e.g., encryption) to address the interception problem, the Examiner's combination still goes against the structural architecture Burger strongly advocated to prevent hacking.

5. The Examiner also gave no consideration to Applicants' section 1.132 evidence.

On June 24, 2004, Applicants filed a 37 CFR 1.132 Affidavit from David M. Tumey, one of the inventors, together with 10 documentary exhibits. This affidavit both described the teachings of the closest prior art – and how it taught away from the claimed invention – and described certain unappreciated advantages of the claimed invention.

Mr. Tumey (today the sole or joint inventor of over 30 issued U.S. patents) described two dominant categories of smart-card based biometric security systems – (1) conventional, and (2)

---

[15] *In re Haruna*, 249 F.3d 1327, 1335, 58 U.S.P.Q.2d 1517 (Fed. Cir. 2001) (quoting *In re Geisler*, 116 F.3d 1465, 1469, 43 U.S.P.Q.2d 1362, 1365 (Fed. Cir. 1997)).

[16] *In re Haruna*, 249 F.3d at 1335 (quoting *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 1360, 52 U.S.P.Q.2d 1294, 1298 (Fed. Cir. 1999)).

match-on-card (MOC) based systems. *See* Affidavit ¶¶ 30-39. In both categories, the user's biometric template is stored on the smart card.

In conventional systems – which include Burger's architecture – a separate biometric capture device is installed at the point of access to capture a fresh biometric image, and authentication or verification is performed off of the card, either by the card reader or a computer linked to the card reader. *Id.* ¶ 30.

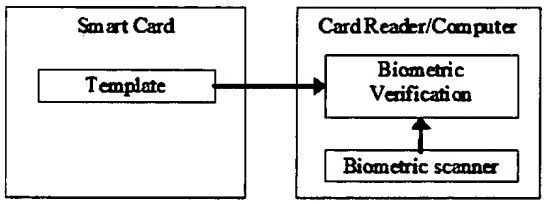
More recently, MOC systems have come into vogue. In MOC systems, circuitry on the card itself compares the template stored in the card with a freshly-captured biometric scan that has either been transferred to the card from an outside scanner or generated from a scanner embedded in the card itself. U.S. Patent No. 5,623,552 to Lane may well have been a harbinger of MOC technology. Lane taught the use of a self-authenticating card that stored prerecorded biometric information (i.e., a template), included a fingerprint sensor *on the card* to capture a fresh biometric, *and* included the processing circuitry to match the freshly sensed fingerprint with the stored template *on the card.* In short, Lane kept everything – the template, the sensor, and the verification circuitry – self-contained on the card itself.

In addition to Lane, Mr. Tumey identified and described several other articles discussing the state of the art of MOC technology. *See* Affidavit ¶¶ 40-48. **Four** different MOC references – the Lane patent itself, an article entitled *Gemplus implements Verdicom's fingerprint matching algorithm on a smartcard* (*see* Affidavit Exhibit 8), an article entitled *The Match On Card Technology* (*id.* Exhibit 9), and an article entitled *Biometrics and Cryptography: Match On Card Paves the Way to Convenient Security* (*id.* Exhibit 10)[17] – all taught away from transferring templates from smart cards to card readers for off-card matching. Lane was critical of

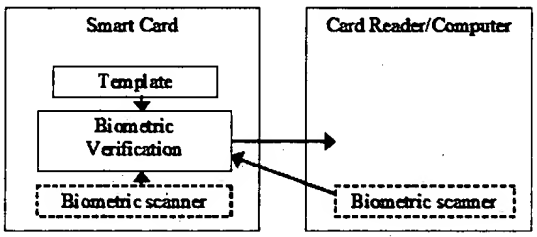
[17] The latter three references post-date the Application. Although they do not constitute prior art, they do reflect the emerging consensus thinking of skilled artisans in the field shortly after the application was filed.

identification cards that transmit sensitive information that could be intercepted. Col. 2, lines 2-7. The *Match On Card Technology* article urged that "[t]he only way to ensure that security is kept is to never let the biometric template leave the closed environment." *See* Affidavit ¶ 44. The *Gemplus* article also cited the MOC feature as an important security advantage: "Fingerprint matching operations are entirely conducted on the smartcard itself in less than a second, unlike previous fingerprint authentication methods that required transfer of template information to a personal computer or workstation for matching leaving a potential security gap." *See* Affidavit ¶ 47. The *Biometrics and Crypography* article stated that "[i]n theory, the best possible solution for combining biometry and digital signatures is obviously devices which bring together the signature function, key memory, and biometric sensor (including the verification algorithm) in one single case which is protected against interference.... The ideal model for this type of device would be, for example, a smartcard with an integrated fingerprint sensor." *See* Affidavit ¶ 40.

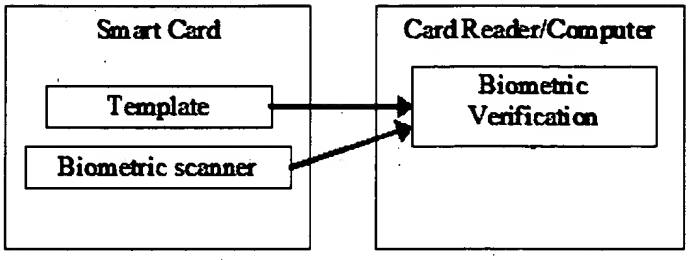
The Applicants' claimed invention, by contrast, does not fit either of these two dominant categories. The differences between Applicants' claimed invention and these two dominant categories is illustrated diagrammatically below:



Conventional Smart-Card Systems



Match-On-Card Systems



Claimed System

As seen above, rather than fitting either of the two dominant categories, Applicants' invention fills an undiscovered and un-suggested niche between these two categories. Neither the conventional smart-card references (e.g., Burger), the match-on-card references (e.g., Lane), nor Morinaga provide any motivation, suggestion, or teaching for filling this niche. On the contrary, both Burger and (especially) the MOC references teach away from Applicants' invention.

The Applicants' invention also provides certain advantages over both conventional smart-card systems and MOC systems. Two of the advantages the invention has over conventional smart-card systems (advantages that would be shared by MOC systems) is that by incorporating the biometric sensor in the card or other portable personal identification device, the point of access security system is made less vulnerable to (1) acts of vandalism that could temporarily disable the entire authorized user population from obtaining access and (2) efforts to spoof the biometric scanner using, for example, a photograph of a face image. *See* Affidavit ¶ 53. The invention also has several advantages over MOC systems. With the claimed invention, different point of access systems can be calibrated to different levels of security (and corresponding false acceptance and false rejection rates), depending on the security needs. Indeed, different point-of-access systems may even use different matching algorithms depending on security needs. These algorithms can also be upgraded without updating the smart cards themselves. *See* Affidavit ¶ 55. Another advantage, cited on page 6 of the application itself, is that by placing a camera in

the smart card, the user's very act of inserting the card into a properly designed docking station will naturally cause the user to look in the right direction, enabling the system to acquire a good-quality facial image of the human user "without requiring attentive action by the human user." Page 6, lines 13-14. The sum of these advantages make the Applicants' invention superior, for certain applications, to conventional and MOC-based systems.

The Examiner dismissed Tumey's affidavit evidence entirely, stating that he did not find these advantages to be unexpected. Final Office Action, at ¶ 2. But the patentability of Applicants' invention does not stand or fall on the presence of unusual or surprising results. The Federal Circuit and its predecessor courts "have considered and rejected the notion that a new result or function or synergism is a requirement of patentability."[18] As the Federal Circuit explained in *Chore-Time Equip., Inc. v. Cumberland*, such a requirement has no basis in the text of the Patent Act:

> A requirement that an invention reflect 'synergism' or achieve a 'synergistic result,' before it may be held patentable appears nowhere in the statute, 35 U.S.C. The test of obviousness under 35 U.S.C. § 103, as the statute makes plain, is whether the invention as a whole would have been obvious at the time it was made to one of ordinary skill in the art.[19]

Furthermore, Tumey's affidavit was not solely directed to the issue of unexpected advantages. The chief purpose of the affidavit was to describe the distinctive aspects of the invention within the context of a much broader scope of the relevant art. What Tumey's affidavit underscores is how the teachings of the closest prior art and articles discussing the most prevalent systems used today are directed *away* from, not *toward*, the claimed invention.

The Examiner simply did not give fair and adequate consideration to Tumey's affidavit evidence. Instead, the Examiner summarily dismissed the Affidavit as "fail[ing] to provide any

---

[18] *American Hoist & Derrick Co. v. Sowa & Sons, Inc.*, 725 F.2d 1350, 1360, 220 U.S.P.Q. 763 (Fed. Cir. 1984).

[19] *Chore-Time Equip., Inc. v. Cumberland*, 713 F.2d 774, 781, 218 U.S.P.Q. 673 (Fed. Cir. 1983).

factual documented proof to support his claims, which are only his opinions." Final Office Action, at ¶ 2. In *In re Mageli*,[20] the Court of Customs and Patent Appeals held that evidence bearing on issue of nonobviousness "is never of 'no moment', is always to be considered and accorded whatever weight it may have." But the Examiner's conclusion entirely disregards the ten references attached to the Affidavit which provide evidentiary support for Mr. Tumey's insights and opinions.

6. *The combination of Burger with Morinaga does not teach storing multiple facial image biometric templates of the same individual on the portable personal identification device (claim 10).*

Claim 10 is separately patentable over the recited combination of Burger with Morinaga. Claim 10 recites that the "prerecorded representation of biometric data identifying an individual comprises a plurality of facial images of the individual." In other words, claim 10 provides that multiple biometric templates (i.e., multiple facial images) of the same individual are stored on the "portable personal identification device."

Even if Burger and Morinaga are properly combined, the combination does not teach or suggest all the claim limitations.[21] Burger describes only a single stored template on the card. Col. 6, lines 15-16. Morinaga states that "an address table with face images can be prepared," but Morinaga does not teach or suggest storing multiple face images of the *same* individual. Morinaga was directed to making space-saving enhancements to "conventional" "portable electronic information devices." Col. 1, lines 11-31. The most *conventional* of such devices as of 1997 – Morinaga's priority date – were PDAs, whose most basic and predominant function, at the time, was to store *contact* information for *multiple* individuals.

---

[20] 470 F.2d 1380, 1383, 176 USPQ 305, 307 (C.C.P.A. 1973).

[21] *See In re Gulack*, 703 F.2d 1381, 1385 n. 9, 217 U.S.P.Q. 401 (Fed. Cir. 1983); *In re Royka*, 490 F.2d 981, 985, 180 U.S.P.Q. 580 (C.C.P.A. 1974) (obviousness requires a suggestion of all limitations in a claim); *accord, CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342, 68 U.S.P.Q.2d 1940 (Fed. Cir. 2003).

7. The combination of Burger with Morinaga does not teach storing different types of biometric templates of the same individual on the portable personal identification device (claim 11).

Claim 11 is also separately patentable over the recited combination of Burger with Morinaga. Claim 11, which depends from claim 3, recites that different types of biometric template information (e.g., fingerprint *and* facial images) are stored on the "portable personal identification device." 127.

Even if Burger and Morinaga are properly combined, the combination does not teach or suggest all the claim limitations. Although Burger teaches *alternative* forms of biometric identification, it never suggests using multiple forms of biometric identification together. Burger teaches using fingerprint verification, or "*[a]lternatively*, retina scan, voice identification, saliva, DNA, *or* other biometrics may be used *instead of the fingerprint*." Col. 4, lines 31-33. Morinaga does not teach biometric identification of any kind. Thus, the references, in combination, do not teach or suggest all of the claim limitations.

B. Claim 12 is patentable over Burger in view of Morinaga and in further view of Pare, Jr., because there is no motivation, teaching, or suggestion to combine Burger, Morinaga, and Pare in the manner claimed.

Claim 12 depends from claims 10 and 3, and further recites that the personal identification device is configured to automatically remove underutilized prerecorded representations of facial images. The Examiner rejected claim 12 over Burger in view of Morinaga and in further view of Pare, Jr.

1. Overview of the Pare reference

The Pare Jr. reference is directed to a traditional centralized biometric system in which a master computer maintains a "master user biometric database which contains or stores the biometric samples of all users registered with the identification computer system." *See* Abstract. Pare also describes a plurality of "local computers" that maintain subsets of the biometric

samples stored in the master database. *Id.* Pare notes that when an individual "relocate[s] to another area of the country, the first time that this individual attempts to be identified in a new local computer, the identification process will take longer because the local computer database will not have the individual's biometric samples" until it retrieves them from the master database. Col. 11, lines 32-41. Pare notes that "[a]dditionally, the local computer which the individual used prior to relocating will eventually purge from its records the biometric sample and personal identification code of [a] relocated individual user, freeing up database space as well as speeding up biometric comparisons for other users of the old local computer." Col. 11, lines 45-48.

2. There is no motivation to combine Pare with Burger and Morinaga in the manner claimed.

There is no motivation, teaching, or suggestion for combining Pare with Burger and Morinaga. Burger taught comparisons between a *single* template stored on a card (not multiple templates from multiple users stored on a database) and the freshly-acquired fingerprint scan. Because Burger is not directed to a traditional, centralized biometric system, Burger presented no need to purge biometric templates. As for Morinaga, it is not even directed to biometric identification, so it supplies no motivation for appropriating Pare's teachings.

The Examiner argued that the motivation to combine Pare with Burger and Morinaga was supplied by "the desire to free up database space and speed up biometric comparisons." *Final Office Action*, at ¶ 4. But purging the *single* template stored on Burger's card would not speed up biometric comparisons – rather, it would render the biometric comparison impossible. The comparison *requires* at least one template! And assuming that there is some "desire to free up database space" on a Burger's smart card, what purpose would it serve to purge the *single*

template stored on Burger's smart card? Burger's smart card would no longer function for its intended purpose.

Furthermore, Pare teaches that "should [the] individual for example relocate to another area of the country," the individual will have to obtain access through a different local computer. Col. 11, lines 32-36. In other words, Pare's local computers are stationary. They do not travel with the user. The fact that individuals relocate, but Pare's local computers do not, provides Pare's motivation for purging a relocated individual's records. But claim 12 is concerned with a "personal identification device" that a user carries with him from one location to another, not a stationary computer dedicated to controlling access to a system. And claim 12 is not concerned with purging the "personal identification code," as does Pare – only underutilized facial images of the card owner. Pare does not provide any suggestion or motivation for purging the underutilized facial images of a user (and not the user's entire identity) from a smart card.

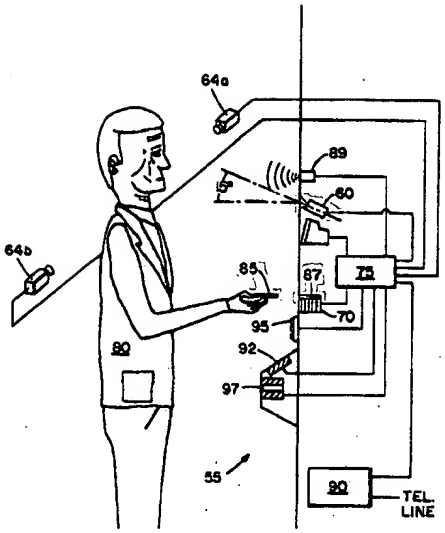
C. Claim 13 is patentable over Burger in view of Morinaga and in further view of Tal because there is no motivation, teaching, or suggestion to combine Burger, Morinaga, and Tal in the manner claimed.

Claim 13 depends from claims 5, 4, and 3, and further recites that the docking station and sensor on the smart card are positioned to facilitate a good quality facial image capture of a user during routine insertions of the smart card into the docking station. The Examiner rejected claim 13 over Burger in view of Morinaga and in further view of Tal.

1. Overview of the Tal reference

Tal teaches a conventional smart card face-recognition system comprising a smart card 85 which contains "facial parameter identification information," an off-card camera 60 for capturing a fresh facial image, and an "information processing means 75" for comparing the biometric template on the card 85 with the facial image captured by the camera 60.

FIG. 3



2. There is no motivation to combine Burger, Morinaga, and Tal in the manner claimed.

The Examiner's rejection of claim 13 fails because there is no teaching, motivation, or suggestion for combining Burger and Morinaga to meet the limitations of the base and intervening claims (i.e., claims 3-5). If claims 3-5 are valid over the Burger/Morinaga combination, then claim 13 is also valid. Tal's teachings do not in any way supply the missing motivation with respect to the limitations from the base and intervening claims.

Tal does provide motivation for positioning the camera of a *conventional* smart-card system at an angle and location that would facilitate a good quality facial image capture. But Tal does not provide any motivation for placing the camera on the card itself, as claimed.

D. Claim 14 is patentable over Burger in view of Morinaga and in further view of Turk because there is no motivation, teaching, or suggestion to combine Burger, Morinaga, and Turk in the manner claimed.

Claim 14 depends from claim 3, and further recites that the sensor is an image-capturing device operable to capture at least two facial images of the individual, and wherein the processor is configured to compare the two facial images to detect motion. The Examiner rejected claim 13 over Burger in view of Morinaga and in further view of Turk.

1. Overview of the Turk reference

Turk discloses "an audience monitoring system 2" having "a video camera 4, which is trained on an area where members of a viewing audience generally sit to watch the TV." Col. 3, lines 17-20. The "recognition system for identifying members of an audience" includes "an imaging system which generates an image of the audience; a selector module for selecting a portion of the generated image; a detection means ... to determine whether an image of a person is present; and a recognition module responsive to detection means for determining whether a detected image of a person ... resembles one of a reference set of images of individuals." *See* Abstract. Turk is not concerned with smart-card based biometric verification systems.

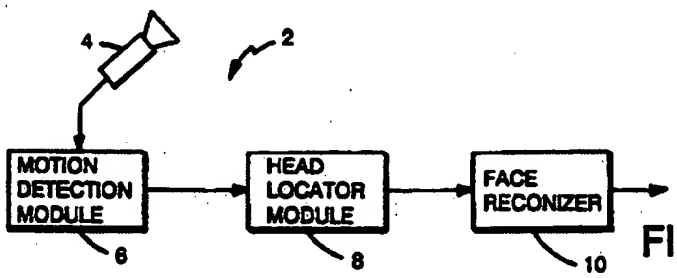


FIG. 1

Turk states that "[w]hen movement is identified" by the motion detection module 6, then "a head locator module 8 selects a block of the image frame containing the movement and sends it to a face recognition module 10 where it is analyzed for the presence of recognizable faces." Col. 3, lines 37-41.

2. There is no motivation to combine Burger, Morinaga, and Turk in the manner claimed.

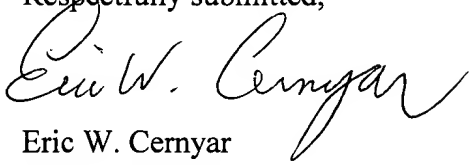
The Examiner's rejection of claim 14 fails because there is no teaching, motivation, or suggestion for combining Burger, Morinaga, and Turk to meet the limitations of the base claim (i.e., claim 3). Even assuming that Turk provides motivation for comparing successive frames of a video capture in order to detect motion, Turk does not in any way provide the motivation to

combine Burger and Morinaga together to meet the limitations of the base claim. In short, if claim 3 is valid over the combination, so is claim 14.

X. CONCLUSION

In view of the foregoing arguments, Applicants respectfully ask that the rejections be reversed and the claims passed to issue.

Respectfully submitted,



Eric W. Cernyar
Reg. No. 45,919
Gunn & Lee, P.C.
700 N. St. Mary's Suite 1500
(210) 886-9500 (phone)
(210) 886-9883 (facsimile)

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex Parte DAVID M. TUMEY

Appeal No. 2005-_____
Application No. 09/545,336
Filed: April 7, 2000
Group Art Unit: 2623
Examiner: Craig Kronenthal
Title: FACIAL IMAGE VERIFICATION UTILIZING SMART-CARD WITH INTEGRATED VIDEO CAMERA
Confirmation No.: 9586
Attorney Docket No.: 062916.004

CLAIMS AND EVIDENCE APPENDIX

* This evidence was submitted with the Applicants' Request for Continued Examination on June 24, 2004. The Examiner formally acknowledged this evidence in his June 15, 2005, Final Office Action, at ¶ 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex Parte DAVID M. TUMEY

Appeal No. 2005-_____
Application No. 09/545,336
Filed: April 7, 2000
Group Art Unit: 2623
Examiner: Craig Kronenthal
Title: FACIAL IMAGE VERIFICATION UTILIZING SMART-CARD WITH INTEGRATED VIDEO CAMERA
Confirmation No.: 9586
Attorney Docket No.: 062916.004

CLAIMS APPENDIX

1. A non-invasive human user identification and verification system, comprising:

a portable smart card;

a silicon-based video camera embedded within said smart card for gathering facial image data;

a digitizer integrated within said smart card for digitizing said facial image data;

non-volatile storage media for receiving and storing said digitized facial image data;

a smart-card docking station with a port for receiving said smart card and communicating said digitized image data therethrough; and

a communications interface for transmitting said stored digitized facial image data from said docking station to a central processor that is housed in a physical structure separate from said smart card, said central processor being capable of receiving and manipulating said data to produce an output signal for use in the identification and verification of said human user.

2. A method for the identification and verification of a human user, comprising the steps of:

capturing one or more first facial images at a remote enrollment station and digitizing said first facial images for storage in a non-volatile media within a portable smart card;

inserting said smart card with embedded video camera into a docking port; and

capturing one or more second facial images and digitizing and transmitting said second facial images from the smart card inserted in said docking port to a central processor that is housed in a physical structure separate from said smart card, said central processor being capable of receiving and comparing said first and second facial images and producing a signal indicative of recognition or non-recognition of said human user.

3. A human user identification and verification system, comprising:

a portable personal identification device;

a communications port adapted to receive information from the personal identification device, the communications port being external to the personal identification device;

wherein the personal identification device comprises:

a prerecorded representation of biometric data identifying an individual;

a sensor configured to capture biometric data; and

a communications interface configured to transmit information to the communications port, the information including both the prerecorded representation of biometric data identifying the individual and the biometric data captured by the sensor; and

a processor communicatively coupled to the communications port and housed in a physical structure separate from said personal identification device, the processor being configured to process the information transmitted from the personal identification device to the communications port and produce a signal indicative of whether the biometric data captured by the sensor matches the individual identified by the prerecorded representation of biometric data.

4. The human user identification and verification system of claim 3, wherein the personal identification device is a smart card.

5. The human user identification and verification system of claim 4, wherein the communications port is a docking station.

6. The human identification and verification system of claim 3, wherein the biometric data identifying the individual comprises facial image data and wherein the sensor is an image-capturing device.

7. The human identification and verification system of claim 4, wherein the biometric data identifying the individual comprises facial image data and wherein the sensor is an image-capturing device.

8. The human identification and verification system of claim 6, wherein the personal identification device further comprises machine-readable storage media for storing the prerecorded representation of biometric data identifying an individual.

9. The human identification and verification system of claim 8, wherein the storage media comprises non-volatile memory.

10. The human identification and verification system of claim 3, wherein said prerecorded representation of biometric data identifying an individual comprises a plurality of facial images of the individual.

11. The human identification and verification system of claim 3, wherein the personal identification device is configured to acquire and store data representing a plurality of biometric characteristics of a person.

12. The human identification and verification system of claim 10, wherein the personal identification device is configured to automatically remove underutilized prerecorded representations of facial images.

13. The human identification and verification system of claim 5, wherein the docking station and sensor on the smart card are positioned to facilitate a good quality facial image capture of a user during routine insertions of the smart card into the docking station.

14. The human identification and verification system of claim 3, wherein the sensor is an image-capturing device operable to capture at least two facial images of the individual, and wherein the processor is configured to compare the two facial images to detect motion.

Appl. No.	:	09/545,336
Applicants	:	David M. Tumey, Tianning Xu, Craig M. Arndt
Filed	:	04/07/2000
Title	:	Facial Image Verification Utilizing Smart-Card With Integrated Video Camera
TC/A.U.	:	2623
Examiner	:	Ryan Hesseltine
Docket No.	:	062916.004

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AFFIDAVIT OF DAVID M. TUMEY
UNDER 37 CFR 1.132

I, David Malcolm Tumey, being duly sworn, state as follows:

1. I am over 21 years of age and am competent to make this affidavit.

2. I graduated with a Bachelor of Science degree in Electrical Engineering from the University of Massachusetts in 1985.

3. I have close to twenty years experience working in the field of electrical engineering and electro-mechanical research and design, including extensive experience in the design and development of both hard-wired circuits and microcontrollers.

4. Between 1985 and 1992, I worked for the U.S. Air Force as an electrical engineer researching advanced cockpit design and aircraft avionic systems. I contributed to the development of neural-network based control systems for flight simulators that, by detecting a pilot's brain waves and learning associations between the brain waves and movements, enabled pilots to fly the simulator with their thoughts.

5. Since 1992, I have worked as an employee or consultant for various medical device firms helping them develop hardware and software control systems for sophisticated electromechanical medical devices.

6. I am listed as the sole or joint inventor of at least 29 issued U.S. patents and dozens of other foreign patents and foreign and domestic patent applications.

7. I am one of the inventors of the subject matter set forth in U.S. Patent Application No. 09/545,336 entitled "Facial Image Verification Utilizing Smart-Card With Integrated Video Camera."

8. In support of my statements in this declaration, I cite several "white papers," press releases, news articles, and other publications recently retrieved from the Internet and attached as Exhibits to this Declaration.

9. Attached as Exhibit "1" is: Lisa Thalheim et al., *Body Check: Biometric Access Protection Devices and their Programs Put to the Test* (dated November 2002) (hereinafter "Thalheim Article").

10. Attached as Exhibit "2" is: Ton van der Putte & Jeroen Keuning, *Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned* (Atos Origin publication dated Sept. 21, 2000) (hereinafter "Atos Origin Paper").

11. Attached as Exhibit "3" is an October 2002 article retrieved from http://trust.ncms.org/MfgTrust1002.htm by the NCMS InfraGard Manufacturing Industry Association Infrastructure entitled *Biometrics and Your Privacy: What's All the Fuss About?* (hereinafter "Privacy Article").

12. Attached as Exhibit "4" is a New York Times article dated March 14, 2003, by Barnaby J. Feder entitled *Face-Recognition Technology Improves* (hereinafter "Feder Article").

13. Attached as Exhibit "5" is a CNET article dated November 1, 2001, by Stefanie Olsen and Robert Lemos entitled *Can face recognition keep airports safe?* (hereinafter "Olsen Article").

14. Attached as Exhibit "6" is an article by Ryan Hay dated November 12, 2003 entitled *Physical Security: A Biometric Approach* (hereinafter "Hay Article").

15. Attached as Exhibit "7" are press releases from Baran Advanced Technologies, Ltd. ("Barantec") spanning the last two years (hereinafter "Barantec [*date*] Press Release").

16. Attached as Exhibit "8" is a May 2000 article from the Industry Journal for Security Professionals entitled "Gemplus implements Verdicom's fingerprint matching algorithm on a smartcard" (hereinafter "Gemplus Article").

17. Attached as Exhibit "9" is: Magnus Pettersson, *The Match On Card Technology* (Precise Biometrics White Paper dated August 22, 2001) (hereinafter "Precise Biometrics White Paper").

18. Attached as Exhibit "10" is: Richard Aufreiter, *Biometrics and Cryptography: Match On Card Paves the Way to Convenient Security* (Utimaco Software White Paper dated July 16, 2001) (hereinafter "Utimaco White Paper").

19. I do not know when the aforementioned papers were first "published" for purposes of determining whether they are prior art. All of these papers are dated after the priority date of the attached application, so they do not themselves constitute "prior art." Nevertheless, they reflect the understandings of many persons of ordinary skill in the art within one to four years of the filing date of the application. They also document many of the problems and long felt needs of the prior art.

20. I commend the Examiner for his admirable and effective job at identifying relevant prior art references. In my opinion, the best and probably "closest" piece of prior art the Examiner has identified is U.S. Patent No. 5,623,552 to Lane.

21. In my view, the relevant art consists of biometric-based access control systems. In my view, the most relevant art, for purposes of my pending application, falls into three dominant categories.

22. To the first category belong the simplest and most conventional biometric access systems, which use a computer or mainframe and a biometric template database. Several users' templates (say "N" templates) are stored in the database. A user identifies itself to a target system by providing the required biometric. The target system then performs an authentication or verification routine to see if there is a match. The use of smart cards and personal identification numbers (PINs) are optional, but not required, for this category. *See* Utimaco White Paper, at 8. I refer to this first category as "**early generation**" devices.

23. One of the disadvantages of all biometric devices, especially "early generation" devices, is choosing the balance between false positives and false negatives. The Atos Origin article introduces this problem nicely: "When a biometrical verification is to occur, a scan of the biometrics of a person is made and compared with the characteristics that are stored in the profile. In general, a certain margin of error is allowed between the observed and stored characteristics. If this margin is too small, the system will reject a righteous person more often while if this margin is too large, malicious persons will be accepted by the system. The probabilities that a righteous person will be rejected and that a malicious person will be accepted, are called *False*

Reject Rate (FRR) and *False Accept Rate* (FAR) respectively. When using a biometric system, one would of course want to minimise both rates, but unfortunately these are not independent. An optimum trade-off between FRR and FAR has to be found with respect to the application." Atos Origin Paper, at 4; *see also* Thalheim Article, at 1.

24. The FRR/FAR problem is exacerbated in systems that try to match a user against a database of many authorized users. The larger the number of authorized users, the higher the FAR, because a malicious user's biometric is more likely to fall within the collective margins of error of many biometric templates than within the margin of error of a single biometric template. The Privacy Article reports that "[w]hen the implications of false results are very serious, then the 1:N identification systems are at their worst. Dr. Philip Agre of UCLA points out ... that face recognition is nearly useless for the application that has been most widely discussed since the September 11th attacks on New York and Washington: identifying terrorists in a crowd. The reasons why are statistical – a 99.99 percent accurate system that scans 10 million faces will produce 999 errors for each correct match of a real terrorist." The Privacy Article also notes that "99.99% accuracy is overly optimistic. According to experts, facial recognition has only about an 85% success rate for matching, while fingerprints range close to 99% accuracy." Privacy Article, at 2.

25. The Olsen Article reports that a Department of Defense study "recorded a high rate of error" in 1:N facial recognition systems "when identifying suspects – even under ideal settings such as scanning a person's image under bright lights, face forward. The study showed a large number of 'false positives,' wrongly matching people with

photos of others, and 'false negatives,' missing people not in the database." Olsen Article, at 2.

26. A 2003 report from the National Institute of Standards and Technology reports that even the best facial recognition systems "made correct matches to the database of images just 50 percent of the time." Feder Article, at 1. For systems employing "reasonable controlled indoor lighting," the best systems had a FRR of 10% and FAR of 1%. Feder Article, at 2.

27. Another disadvantage of all biometric scanners, especially those employed in "early generation" devices, is the ease with which they can be fooled with a dummy (e.g., an image or latex reconstruction of a fingerprint). The authors of the Atos Origin article tested several commercially available fingerprint scanners and warned that "to the knowledge of the authors, none of the fingerprint scanners that are currently available can distinguish between a finger and a well-created dummy." Atos Origin Paper, at 7. Fingerprints are easily duplicated and "[o]ne of the best ways to obtain such a print," say the authors, "could be the fingerprint scanner itself." Atos Origin Paper, at 8. The authors of the Thalheim article were also able to fool several fingerprint devices by a variety of methods. Thalheim Article, at 5-9. They were able to gain access to one system simply by breathing on traces of fat left by prior fingerprints on the sensor's surface. *Id.* at 5. They also fooled facial recognition systems with still and motion pictures displayed on a computer notebook. *Id.* at 4.

28. A third problem with this first category is the ability to breach security through multiple retries. A malicious user who is denied access can keep retrying a system until it is allowed access. Thalheim Article, at 4.

29. A fourth problem with the first category (and indeed, also with the second category described below) is the opportunity to vandalize a common, publicly accessible biometric sensor placed at a point of access. This can be done, for example, by breaking or damaging the sensor or camera, painting over the lens, or placing chewing gum on the sensor. Barantec's November 15, 2002 Press release reports that "[i]n the past, the security industry has used stand-alone proximity units and avoided mechanical keypads in high traffic areas, which are susceptible to vandalism, excessive use and the elements." Barantec's January 5, 2004 Press release reports "a vulnerability with mechanical and membrane keypads ... It was not so much that the sensor would fail and someone would get inside but that someone could damage the fingerprint lens and cause failure."

30. In the second category, the user's biometric template is stored on a card or portable device carried by the user. A separate biometric capture device, installed at the point of access (e.g., on an ATM machine, the entryway to a secure facility, next to a computer terminal), is used to capture a fresh biometric image from the user and scan the biometric template stored on the user's card. Both the template from the card and the image from the reader are transmitted to a computer (not on or part of the card) with which the reader is in communication, which performs the authentication or verification. I refer to this technology as "**conventional smart card technology**."

31. Conventional smart card technology addresses the 1:N problems of the first category of biometric access devices, because a user's biometric need be compared with only a single authorized user's biometric template(s). It also makes it somewhat more difficult for a malicious user to gain access with a well-created biometric dummy,

because the malicious user not only needs the biometric dummy, but also an authorized user's smart card, to gain access to the system.

32. Conventional smart card technology does not, however, solve the vandalism problem described above, because the biometric scanner is maintained at the point of access.

33. Furthermore, conventional smart card technology is also vulnerable to security breaches through, for example sniffing or data snooping. A malicious user may use a sniffer to capture and store the template transmitted by the card and reuse the template, together with other known techniques to spoof the point-of-access biometric scanner, to breach security. *See* Thalheim Article, at 2, 12-13.

34. Recently, a new category of art – referred to as "**match on card**" (or "**MOC**") technology – has developed. U.S. Patent No. 5,623,552 to Lane may very well be considered a harbinger of MOC technology.

35. In MOC technology, a smart card is used not only to store a user's reference biometric template, but also to perform the matching function. If a match is found, the smart card releases or transmits information, such as (in Lane's case) credit card information or (more recently) an encryption key for use in a public/private encryption key authentication system. *See* Precise Biometrics White Paper, at 3; Utimaco White Paper, at 9-11.

36. Whether Lane's disclosure, based on an application filed in January of 1994, was sufficient to enable MOC systems or whether then-existing technology was feasible to make them operable in accordance with Lane's teachings is an open question.

37. Page 9 of the Utimaco White Paper claims that the "[f]irst technology demos of this ["match-on-card"] principle were presented at the CeBIT 2000 trade fair" and that "[s]martcards with this functionality have been commercially available since the end of the year 2000."

38. Another article announced one company's implementation of MOC technology using a fingerprint matching algorithm in May 2000, referring to it as a "breakthrough." *See* Gemplus Article.

39. But the earliest of these MOC smart card devices did not even incorporate a biometric sensor. Rather, they loaded the biometric information from a reader at the point of access. Precise Biometrics' White Paper claims that "[t]he ideal solution for secure biometric verification would be that the fingerprint scanning and the matching were done on the same component." But the article, written on August 22, 2001, observed that "[t]oday, no such device exists." Precise Biometrics White Paper, at 3.

40. Likewise, the Utimaco White Paper claimed that "[i]n theory, the best possible solution for combining biometry and digital signatures is obviously devices which bring together the signature function, key memory and biometric sensor (including the verification algorithm) in one single case which is protected against interference. . . . The ideal model for this type of device would be, for example, a smartcard with an integrated fingerprint sensor." But it too observed that "[t]hese devices [using an integrated fingerprint sensor] are currently being developed by various manufacturers" and have not yet become cost-effective. *See* Utimaco White Paper, at 11.

41. The Hay article, dated November 12, 2003, reports that Hewlett-Packard "became the first manufacturer to add biometric identity checking to a mass-market

consumer portable electronics device last year, when it built a small fingerprint scanner into its HP IPAQ H5450 PDA." Hay Article, at 4.

42. Lane and these succeeding MOC references teach away from smart cards that transfer template information to a personal computer or workstation for matching.

43. Lane's first noted object is "to provide an identification card which does not require external equipment for identity verification." Col. 2, lines 10-13. Lane is also critical of identification cards that transmit sensitive information (which would include a biometric template) that could be intercepted. Col. 2, lines 2-7.

44. The Precise Biometrics White Paper is steadfastly critical of smart cards that transfer template information to a personal computer or workstation for matching. "To gain maximum security, the biometric template must be stored securely in a closed environment. If the biometric matching procedure is performed outside this closed environment it is exposed to the open environment, where anyone could steal the template. Even if the fingerprint template is protected by another security mechanism this is to be viewed as the weakest link, and the biometrics does not really add any security. The only way to ensure that security is kept is to never let the biometric template leave the closed environment. In this case the biometric matching has to take place in this closed environment as well." Precise Biometrics White Paper, at 2.

45. The paper again reiterates that "The most important thing is that the stored template must never be exposed." Precise Biometrics White Paper, at 3.

46. Again the paper urges that "[t]he only way of securing a smart card with biometrics is to let the match take place in the smart card itself, where the biometric template is stored. If the match is performed outside the smart card there has to be some

message sent to the card to unlock it. That message has to be created outside the card, and then the biometrics really doesn't add any security." Precise Biometrics White Paper, at 6.

47. The Gemplus Article is also critical of smart cards that transfer template information to a personal computer or workstation for matching. The article states that "[f]ingerprint matching operations are entirely conducted on the smartcard itself in less than a second, unlike previous fingerprint authentication methods that required transfer of template information to a personal computer or workstation for matching leaving a potential security gap."

48. In summary, Lane and succeeding MOC art strongly teach away from the claimed invention, which utilizes a portable device (such as but not, unless expressly so stated, limited to a smart card) to capture a fresh biometric and transfer it, along with the template (or some processed or coded version of it) to an external device for matching and verification.

49. None of the Examiner's cited references, and none of the references cited in this declaration, express any appreciation or understanding of any advantages to be obtained from the claimed system over both conventional smart card technology and MOC technology.

50. In his Advisory Action, the Examiner made the following observation: "The examiner would also like to point out that applicant has not mentioned any particular advantage to performing the verification separately from the portable personal identification device (smart card)."

51. It should be apparent, then, that any advantages to the claimed invention are not obvious.

52. I respectfully submit that the claimed combination has important "unexpected advantages." Namely, the claimed invention combines several advantages of the first, second, and third categories which, as shown above, the general art has treated as mutually exclusive benefits that must be traded off depending on what system is chosen.

53. One advantage of the claimed invention over the first and second categories of biometric access systems mentioned above is protection from vandalism. By incorporating a biometric scanner (such as a camera) in the portable personal identification device, the point of access security system is made less vulnerable to acts of vandalism that could temporarily disable the entire authorized user population from obtaining access. Granted, a malicious user could steal a card and vandalize the scanner on the card itself, but this would only disable the card, not the entire access system. Furthermore, authorized users are somewhat likely to try to protect their card.

54. Another advantage of the claimed invention over the first category is that it facilitates 1:1 matching, with its lower FRR and FAR rates compared to 1:N matching systems.

55. The claimed invention is also superior to MOC systems (the third noted category of art) in at least one obscure, unappreciated, and therefore unexpected way. With the claimed invention, different point of access systems can be calibrated to different levels of sensitivity (and corresponding FRR and FAR rates), depending on the security needs. Indeed, different point of access systems may even use different

matching algorithms depending on security needs. And with improvements in technology, these algorithms can be upgraded without updating the smart cards themselves.

56. The aforementioned advantages should be considered not in isolation, but in combination. Considered only in isolation, each of the advantages cited above favor what has been treated in the art as mutually exclusive categories of biometric systems. An unexpected advantage of the claimed invention is that it combines the aforementioned advantages into one device.

David M. Tumey

STATE OF TEXAS §
COUNTY OF BEXAR §

BEFORE ME, the undersigned authority, on this day personally appeared DAVID M. TUMEY, known to me to be the person of that name, who signed the foregoing instrument, and acknowledged the same to be his free act and deed.

GIVEN under my hand and seal of office this 22 day of June, 2004.

JANIS DEITZ
My Commission Expires
September 25, 2007

Notary Public

JANIS DEITZ
Printed Name of Notary

Commission Expires 9.25.07

In German language

Aktuelles Heft

Support
Hotline & FAQ
Tipps & Tricks
Treiber & BIOS
Firmenkontakte

Download
Software zu c't
Free- & Shareware
c't-Projekte
Testbilder & Vorlagen

Service
Tipp-Datenbank
c't-CD-Register
Internettarife
Telefontarife
Virenschutz
Flohmarkt

Magazin
Heftarchiv
c't specials
English Pages
Benchmarks
Red. Stuff
Leserforum
c't-Bildmotive
URLs aus c't
Schlagseite

Aktionen
Browsercheck
Krypto-Kampagne
Schulen ans Netz
Netz gegen Kinderporno
TV/Radio-Termine

Abo & Heft
Mediainfo
Kontakt
Impressum

c't 11/2002, page 114 - Biometrie

Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler

Body Check

Biometric Access Protection Devices and their Programs Put to the Test

Memorizing passwords is out. Laying your finger on a sensor or peering into a webcam can suffice to gain you immediate access to a system. There is the danger, however, that this new ease might be bought at the expense of security. How well do biometric access controls prevent unauthorized access? We have tested eleven products for you.

According to estimates of the IBIA, the international organization of biometric devices and programs suppliers, worldwide turnover of biometric security devices and programs this year will for the first time exceed the 500 million euro limit. Though the growth is primarily being driven by large scale orders by industrial customers and administrative bodies, nevertheless the number of products on the market designed for in-home and in-house PC use is rising.

The range of biometric security access tools for PCs meanwhile extends from mice and keyboards with integrated fingerprint scanners to webcam solutions whose software is able to recognize the facial features of registered persons to scanners that make use of the distinct iris patters of humans for identifying individuals. When the PC is booted the security software that goes with the tool writes itself into the log-on routine expanding the latter to include biometric authentication. In many instances the screen saver is integrated into the routine thus allowing for biometric authentication after breaks from work while the PC is still running. Sophisticated solutions, moreover, permit biometrically-based security protection of specific programs and/or documents.

The problem that all biometric security access procedures and devices still have in common, however, is the necessity of establishing fault tolerance limits: When a manufacturer - by making the appropriate hard and software efforts - decides to set his fault tolerance limits very narrowly, this increases his system's security, the user-friendliness of the system, however, is likely to decline in proportion. Should he on the other hand decide from the outset to permit considerable deviation, this will make his system easy to use, but greatly diminish its protective value.

Core Question Unanswered

The studies published to date on questions of biometric security are in the main based on evaluations of the false rejection and false acceptance rates (FRR, FAR) that are so popular with that line of business. In the event of a false rejection a user is prevented from accessing a system despite his or her access authority for the system; the reason usually being that the

biometric features of the user are weakly developed, from the point of view of the system.

A false acceptance incident on the other hand allows a person whose biometric features have not been registered to log-on to the system. In most cases cheap sensor chips or badly implemented security software is responsible for a malfunction of this kind. Generally speaking, however, the statistically determined error probabilities do not give clear answers to the question of whether biometric solutions are able to protect a system even against an assailant bent on overcoming biometic protective measures. Unlike empirical scientific procedure, a hacker is scarcely likely to muster a battery of a thousand experimental subjects in the hope that one of them might perhaps be mistakenly accepted by the system. But the latter is the very core question that a security system must be made to answer.

A fingerprint kit supplied by the regional Criminal Investigation Department of the German federal state of Lower Saxony stood us in good stead.

Although the Fraunhofer Research Institute, based in the German city of Darmstadt, in collaboration with the German Federal Institute for Information Technology Security (BSI) conducted an extensive series of tests last year in the course of which "deliberate" searches for security loopholes in specific system were undertaken, the results, obviously due to pressure from the manufacturers, were never made public. Instead of finally laying its cards on the table, the biometrics line of business prefers to hide behind error rates it has measured itself.

There is thus only one way at present to determine how vigorously the current biometric security systems are able to resist attempts at overcoming them: test-it-, assail-it-, and outfox-it-yourself. Attempts undertaken to breach the systems can roughly be assigned to three different scenarios:

The first approach relies on tricking the biometrics system with the aid of artificially created data whilst making use of the regular sensor technology of the system; a precondition for this approach being spy-work that gets hold of more or less easily obtainable biometric features such as an image of a face or a fingerprint. After developing the appropriate photograph(s) and/or creating the artificial fingerprint(s) required, these copies of features can then be used to attempt to obtain authentication. The reactivating of traces of fat on a fingerprint scanner - of so-called latent images - also belongs to this scenario.

The second scenario also entails tricking the biometrics system with artificial data. In this case, however, by playing back to it reference data sets, collected, for instance, with the aid of a sniffer program listening on the USB port, the system's regular sensor system is bypassed. This procedure is commonly called a replay attack. For more on USB sniffers and hardware analyzers consult the 'Attacking Via the USB Port' box.

The third approach is made up of attacks that aim at the data base directly. In general this scenario requires that one be in possession of data base administrator rights and have permission to exchange sets of data used as reference sets for recognition purposes. In the event that these data sets have no separate protection of their own the assailant has the opportunity of forging user data with a view to reactivating these at a later date in accordance with his or her designs. In the sensitive area of financial transactions this could turn out to be

a ticking time bomb. Vide the hypothetical case of a former bank employee who years after leaving his firm decides to bring back to life the at one time surreptitiously created data set 'Mr. Miller's eleventh finger' with the intention of generously taking care of his retirement needs.

In our attempts at outfoxing the protective programs and devices we have concentrated on the first method: direct attempts at deceiving the systems with the aid of obvious procedures (such as the reactivation of latent images) and obvious feature forgeries (photographs, videos, silicon fingerprints). After already obtaining astonishing results by means of this approach, we conducted exemplary tests only on whether it was possible to extract biometrically-relevant data by eavesdropping on the communication via the USB port between the computer and the sensor.

The Candidates

All eleven biometric protection applications tested by us are products that were presented at this year's CeBIT trade fair at the German city of Hanover and all are freely available on the market. Even though the range of products tested was not complete it did on the whole reflect market conditions: The great majority of the currently available biometrics products relies on features of the fingers for user identification. Neck-and-neck in second and third place are face recognition and iris scanning systems. All other devices and programs such as make use of language recognition, hand geometry measurement, signature recognition or keyboard touch dynamics taken together have only a marginal share of the security biometrics industry's overall turnover.

Besides six products involving capacitive fingerprint scanners (Biocentric Solutions, Cherry, Eutron, Siemens and Veridicom) two optical (Cherry, Identix) and one thermal (IdentAlink) fingerprint reader were available to us. Our tests also took in the Authenticam by Panasonic, an iris scanner that is currently being marketed in the USA and is scheduled to enter the European market in the near future, as well as FaceVACS- Logon, a technical solution for recognizing faces developed by the Dresdner Cognitec AG. Our test environment consisted of three PCs (1-GHz-processors, 128 Mbytes of RAM, 32 Mbyte AGP graphics cards) running Windows 98 and Windows 2000, as well as of a Gericom notebook with a 14" LCD screen running Linux.

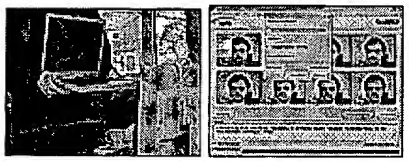
Photo Ops

Compared with other biometrically-based security access procedures the marketing opportunities for facial feature recognition devices and programs are assumed to be fairly good. The technology profits especially from the fact that some of its features are already integrated into the living conditions and habits of PC users: Many people are a good deal more familiar and comfortable with gazing into a camera than, for instance, having their eyes scanned by infrared beams or their fingerprints 'taken' by a device, the latter procedure perhaps awkwardly evoking images of criminal investigations.

Cognitec's FaceVACS-Logon, which can be applied both as a authorization access solution and as a screen saver, uses as its sensor a commercially available webcam. Cognitec recommends Philips's ToUcam PCVC 740K. Authorization proceeds almost automatically: When a person approaches the PC's webcam the recognition software aided by special algorithms in a first step begins to search in the pictures it takes for eyes; once these are found

it mathematically projects based on their coordinates a virtual rectangle into the picture. The following pattern recognition process in the course of which so-called Support Vector Machines (SVM) capture characteristic facial features which are subsequently compared with stored facial patterns takes place within the boundaries thus established. In the event of a positive match the authorized person is granted access to the PC immediately.

Maximum security level not withstanding, FaceVACS-Logon can be outfoxed with a short video clip of a registered person.



During enrollment, i.e. the creation of an initial reference set of facial images, FaceVACS begins by storing a number of images of the new face in the .PPM format in a log file. During each subsequent authentication procedure images, this time with a .fvi tag, are added to the collection. As these image data are neither encrypted nor otherwise particularly protected they can be read and possibly manipulated once access to the system has been acquired. Moreover, the log files allow one to ascertain which are the 'good data' sets, those, in other words, that lie above the recognition threshold. We began our attempts at outfoxing the system by transmitting the freely accessible image files to the notebook. We then presented the images upon the notebook's display to the ToUcam. Once we had found the appropriate distance between the webcam and the display, it would take but one attempt in most cases for FaceVACS-Logon to accept the image presented and hence grant us access to the system.

In the course of our next attempt at trickery we recreated a situation that could easily come about in the real world: An assailant without access to stored data attempting to overcome the obstacle of the facial recognition procedure. For this purpose we 'secretly' took three pictures in all of an authorized user with a simple digital camera under different lighting conditions. These digital images we then again transferred to our notebook, proceeding to show the various images to the webcam via the former's display. The result was that after only two images of the digital camera we had put FaceVACS's biometric protective measures out of action. From then on the system would cede control of the PC to anyone who held the notebook's display up to the webcam's scrutiny.

Playing Video Games

To prevent deception with the aid of photographs Cognitec has integrated a higher level of security known as Live-Check into the FaceVACS's software. Indeed once Live-Check has been activated all attempts at deception with stills (such as those described above) are foiled. On the downside, however, user-friendliness sinks considerably and registered users are only seldom recognized right away.

Hence we simply shot a short .avi video clip with the webcam in which a registered user was seen to move his head slightly to left and right. As brief movements suffice for FaceVACS to consider an object alive and as the program engages in simple 3D calculations only, we were not particularly surprised about the success of our approach: Once the appropriate display-to-ToUcam distance had been found the program did in fact detect in the video sequence played to it a moving 'genuine' head with a known facial metric, whereupon it granted access to the system.

In a worst case scenario this state of affairs implies that a person without a professional background to movie making who had wielded a digital camera during a public meeting and there shot visual material of authorized personnel, to log on to a protected system, need only modify the acquired material slightly and transfer it to a portable PC.

Sleight of Finger

The most common method for distinguishing fingerprints is based on the so-called minutiae, the 'small details'. The minutiae are interruptions to the lines upon the fingertips, such as endpoints, bifurcations, whorls or islets. To identify a human fingerprint unambiguously information about the type, position and orientation of at least ten to twelve of these minutiae is required.

In the main capacitive fingerprint scanners are used to get hold of these minute details -- above all because the CMOS chips used in them have for some time now been available at a fairly reasonable price. When a finger is placed on the device the scanner's 65,000 pixels treat the surface of the skin as a capacitive pole. The capacitance of each miniature capacitor depends on whether a line or a trough is to be found above the measuring point in question. The device then converts these individual values into an 8-bit gray scale, extracts about 20 minutiae and proceeds to store these values in a reference file for future authentication purposes.

Even simple breathing will do the trick of outwitting a capacitive fingerprint scanner.

In Germany the best known among the desktop fingerprint scanners is Siemens's ID Mouse, which is equipped with Infineon's capacitive FingerTIP sensor. In its current Professional V4.0 version the device can, moreover, be used as a optical USB scroll mouse. During the tests there was never a problem with installing the USB drivers and setting up the application software. Under normal conditions the enrollment as well as the subsequent authentication almost always went off quickly and without error.

It was equally easy though to outwit the ID Mouse with simple tricks. Although this according to the manufacturer's statements should have been impossible we were able several times to reactivate by simply breathing upon them traces of fat left by fingerprints upon the sensor's surface, thereby overcoming the biometric protection of the system. We cupped our hands above the scanner and within the shell thus formed breathed gently upon the sensor's surface. Meanwhile on the screen of the biometrically-protected computer we were able to see the contours of an old fingerprint slowly reemerge.

A fingerprint on adhesive film may suffice as a biometric ID.

It was also possible to reactivate latent fingerprints by carefully placing a thin-walled water-filled plastic bag onto the sensor's surface. The advantage of this technique is that the water spreads more evenly across the sensor's surface. When the latent fingerprint was a good quality one few attempts would normally suffice to gain us access to the system. Even when the security mode was set to its maximum (extended mode) we were able to undertake these simple latent image activations at the ID Mouse. The probable reason for this phenomenon being that the capacitators of the capacitive sensor are sensitive to humidity. Damp air that, for instance, condenses on the sensor's surface where there are residues of fat causes the relative dielectric constant on the sensor's surface to change thus leading to a change in capacitance which the device interprets as a release signal inducing it to undertake a measurement.

The ID Mouse can be outfoxed even more easily by dusting the fatty residue of the fingerprint on the sensor with commercially available graphite powder (Ravenol), then stretching an adhesive film over the sensor's surface and gently applying pressure on it. Whereas we were only intermittently successful at overcoming the biometrics barrier when using the breathing or the water bag method our success rate with the adhesive film technique when the latent fingerprints were of good quality was almost one hundred percent.

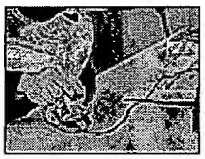
According to Siemens especially designed algorithms of the security software belonging to the package check whether the currently scanned fingerprint in terms of its position and angle coincides within certain predetermined tolerances with the last registered version of the print. This is supposed to prevent the system from being taken in by all attempts based on latent image reactivation or replay.

According to a statement from Munich the company could not conceive of a reason why their procedure should have failed when we tested it. In future, the statement went on, the company would focus even more on the problem of latent image reactivation.

In the course of a further concrete assault approach we acted out a scenario of a theft of data by more professional means, theft of a kind that people engaged in the field of industrial espionage might be thought to be capable of. With the aid a fingerprinting kit that the regional Criminal Investigation Department of the German federal state of Lower Saxony was generous enough to make available to us we took fingerprints from glasses and CDs. We dusted the prints with graphite powder, secured them with adhesive film, and then after placing them on the scanner applied gentle pressure to the surface. Our success rate with this approach was very high, regardless of whether the system was in its normal or its extended security mode.

The Cherry G83-14000 keyboard had a comparable security behavior, which was not hard to predict as the insides of the keyboard scanner and that of Siemens's ID Mouse are identical. The former was thus without much ado outfoxed by the same procedures.

Eutron's fingerprint reader Magic Secure 3100 on the other hand is a product manufactured by the South Korean firm of Hunno and includes a CMOS TouchChip by STMicroelectronics. For covering the European market the Italian firm of Eutron merely relabels this combination of fingerprint scanner and optical USB scroll mouse. It too is a capacitive scanner with properties and weaknesses comparable to the product by Siemens: Approaches to deception via the regular sensory mechanism of the device, of the kinds described above, also lead to success. Though the breathing approach was not quite as reliable, the moment graphite powder came into play we were easily able to gain access to this system also.



Reactivating a latent image can also be done with a little water in a plastic bag.

The only product in the field tested to possess a special protective mechanism for the sensor surface of the capacitive scanner was Veridicom's 5th Sense Combo. A possible solution for this device that might have done away with the latent image problem once and for all after every use would have been to equip the underside of its protective spring-driven sliding cover with a miniature cleaning sponge. Besides the cover Veridicom's fingerprint reader is furnished with an integrated smart card reader. In the case of smart-card biometric-authentication applications the access check routine is no longer confined to the protected computer in question, the user can also seek authentication in relation to reference data stored on the smart card. Alas, Veridicom passed up the design opportunity for wiping away latent images on its device. We were able to outfox the device in much the same way we had outfoxed the others, expect that with the Veridicom scanner there was the slight additional difficulty that it was necessary to hold the sliding cover open with one's other hand or by sticking a matchstick in.

Security Roulette

Completely out of line during out tests were the two PDA solutions by the US American manufacturer Biocentric Solutions. To ensure their integration into the operating systems Windows CE and Pocket PC 2002 both applications make use of the program BioFamily that comes with the devices. Whereas BioHub is designed to prevent unauthorized access to a variety of these little helpers by means of a CompactFlash Card with an integrated fingerprint scanner, naught but Compaq's iPAQs will fit into the BioSentry expansion jacket with its rear FP scanner.

Even during normal use problems with both products kept popping up. Neither BioHub nor BioSentry reliably recognized registered users - a state of affairs that repeated soft- and hardware resets were unable to remedy. Sometimes it took 30 attempts for a simple authentication to succeed, then again placing the very tip of a fingertip of an unregistered user on the sensor's surface would suffice for access to the PDA to be granted. In a nutshell: Since there was no way to sensibly test either BioHub or BioSentry, we put them back where they had come from - inside their FedEx packages.

Illuminating

The second most frequent manner in which fingerprints are currently mechanically scanned is the optical one. In this case the finger which is positioned above a prism or a diffracting grid is illuminated by light from color LEDs and photographed by a CCD or a CMOS camera. An alternative technique consists of placing the finger illuminated from below upon a light-conducting fiberglass surface that is directly linked to a CMOS chip element.

Accordingly, during our tests we were unable by reverting to simple latent image activation to get the better of our candidate, Identix's Bio-Touch USB 200 - with systems of this kind to trigger the recognition procedure at all it is necessary that, prior to the CMOS camera taking the picture presented to it via a concave mirror, the light from the red LED source be reflected by an object on the scanner's surface.

For the first time we thus had to avail ourselves of an 'artificial finger.' An intruder with even minor manual skills might, for example, with the aid of photo-sensitiv lacquer fashion the image of a fingertip into a mould for a three-dimensional likeness of the fingertip in question. As these steps are obvious we felt free under laboratory conditions to take a somewhat simpler approach: We took small common tea-warming candles, removed their wicks, pressed fingertips into the warm wax and proceed to fill the troughs with commercially available silicon.

The moment we placed the thus fashioned 'fingertips' on the scanner's surface BioTouch's resistance collapsed: The DFR-200 optical sensor accepted the silicon copies without hesitation, during authentication as well as during enrollment. The reverse of the deception also worked: When in possession of a silicon copy of a fingerprint of a registered person we were able to log on to the computer 'incognito'.

Moreover, in the course of further experiments we also detected that even without the aid of an 'artificial finger' it was possible to deceive the optical sensor. For we were again able to gain access with our tried-and-tested adhesive film technique. In this case, however, though it was not enough to simply place the film with the graphite pattern on the scanner's surface, once a halogen lamp was made to shine on the scanner from a distance of about 30 centimeters, that too worked. Apparently, the intense back-lighting on the one hand enhanced the contrastive properties of the graphite powder on the scanner's surface whilst on the other inducing a kind of snow blindness in the sensor.

The G81-12000 keyboard made available to us by Cherry is likewise equipped with Identix's optical fingerprint scanner, hence its results vis-à-vis our attempts at deception were more or less identical.

Hot Spots

A lot less frequently than those with capacitive or optical systems are fingerprint scanners with thermal recognition systems deployed. The latter systems measure the minimal temperature differences between the 'hills' (the lines of fingertips) and the 'valleys' (the furrows in between) that the sensor registers on the fingertip's surface.

IdentAlink's Sweeping Fingerprint Scanner FPS100U works on the basis of Atmel's CMOS-Finger-Chip-Sensor FCD4B14, which consists of a total of eight rows, placed one after the other, with 240 sensor pixels each. To trigger the scanning procedure one moves one's finger, applying gentle pressure, slowly across the only about half a centimeter wide thermal sensor.

Located right next to it is a small heating unit that raises the temperature of the lines of the finger while they are moving across the sensor. Immediately after it has been switched on the device cannot supply usable images, only after a short heating-up period can high quality images of fingers be generated.

If the BioLogon software that goes with the device hadn't repeatedly stymied our attempts at getting to grips with it - on occasion the system crashed five times during enrollment and was only 'forced' back into cooperating with us by our pulling the USB plug - IdentAlink's Sweeping Fingerprint Scanner might have made a comparatively good impression during the tests. Because unlike the case with the capacitive and optical sensors owing to the thermal sensors minute surface area it was not possible to reactivate latent images or make use as before of our otherwise so successful adhesive film technique.

Only on the basis of silicon copies of authentic fingerprints were we able to score some successes: With their aid we repeatedly surmounted the biometric-access protection barrier. With a little bit of practice we were able to use silicon copies to create reference data sets and thereafter to gain access with the original finger as well as with the copy of the same.

In conclusion it must be said, however, that the amount of effort required to trick the sensor mechanism of a thermal fingerprint scanner with artificial data is significantly higher than that required in the other cases described above. Nevertheless, even the FPS100U is still a long way off from guaranteeing secure access.

The Highlight

Biometric applications that make use for access control purposes of individual features of a person's eyes, such as those of his or her retina or iris, are somewhat tainted by their cliché association with secret service activities in high-security bunkers. Even though a handy iris scanner for the home already exists: Panasonic's Authenticam BM-ET100, which with its separately operating webcam is not much lager than a pocket-size edition of Shakespeare's sonnets.

The bottom section of the scanner's casing contains three infrared light sources. The two outer and somewhat weaker ones illuminate the iris while the user adjusts his or her distance to the device. When the user gazes straight into the camera from a distance of about half a meter (48 to 53 cm), a mark detectable in the opening of the lens changes from orange to green, at the same time the infrared light source in the middle begins to shine brightly and a sufficiently high quality picture of the iris is taken by the camera.

At first the Authenticam presented us with quite a challenge. During our first attempts at trickery we offered digitally-shot iris images via the notebook display as well as via a head-mounted display (HMD) to the black and white video camera of the scanner; owing to the too intense reflection of light on the displays without success, however. Due to the overexposure that resulted the system was also unable to recognize the features of iris images that had been printed on normal paper.

What was interesting though was that all iris images taken by the system showed a bright spot in the middle of the pupil. This fact gave us the idea that - besides fulfilling the requirement of acquiring a green light by the system - we might in our next attempt at outwitting it show the system's camera human digital iris images printed on paper that had a small hole cut into

the middle and behind which were placed the hidden pupils of actual human beings.

A sight for sore eyes perhaps, but very effective: achieving authentication with someone else's iris by hiding your own pupil behind it.

It quickly became apparent that this would be the way to success. As an opening to its calculations the PrivateID software by Iridian that comes with the device requires the in-depth aperture of the pupil, upon the center of which it bases its computations of the iris. By doing the deed we had at least initiated the taking of images by the system.

The only thing that was still missing was a printed picture of an iris with an appropriate degree of quality. Hence we presented to the Authenticam a digital image of a human eye that had been sprayed onto mat inkjet paper with a resolution of 2400 x 1200 dpi and into which we had previously cut a miniature hole. This was enough to overcome Authenticam's resistance: We were granted access to the system under the assumed identity of 'Master False Eye'.

It was also possible to enroll with the aid of the 'artificial' eye. From that point onwards anyone in possession of the eye pattern was able to log on to the system. Moreover, the person whose eye had been used to create the pattern was also able to acquire authentication in relation to the picture-generated reference data set with his own live iris.

Panasonic on account of these results, as was to be expected, proved to be 'not amused'. We were told that the product made available to us for our tests was a prototype which would be redesigned prior to its introduction to the German market. As the system has been marketed in the USA for some time now, we suspect that without our tests no such redesigning would have been contemplated. It has to be said in favor of the iris scanner, however, that under real life conditions it would not be easy to obtain iris images of authorized persons. With such images at one's disposal, however, creating a deceptive eye-patch can no longer be thought of as much of a problem as high resolution inkjet printers and mat paper cannot today be considered high-tech equipment.

Conclusions

For fairness' sake we need to emphasize again at this point that according to their manufacturers' statements none of the products tested by us was designed for use in a high-security environment. Nevertheless, the question can be put whether a security application whose protective measures can be foiled with the simplest of tricks is an investment of 300 euros worth making.

A question also raised by our tests is whether the expensive systems are really more secure than the ones tested by us - or whether it is simply the case that no one has yet seriously tested them? After all, the weaknesses are in part those of the algorithms used and not those of the sensors applied. Should better algorithms already exist, why do the manufacturers not use these for their low-priced products also? The development cost argument does not apply

to software that already exists.

Even though manufacturers of biometric products can scarcely avoid for marketing reasons extolling their applications as mature and secure: The technology suitable for mass consumption for identifying and authenticating the identity of persons on the basis of their physical features is obviously still in its infancy.

That much remains to be done, before any abolition of passwords or PINs in favor of biometric procedures can even be contemplated, our tests have shown: We were able, aided by comparatively simple means, to outwit all the systems tested. Whether silicon or a notebook constitute the kind of unusual 'high-tech weaponry' that some company statements made in response to our results claimed we had used, is up to the reader to decide. The fact remains, however, that the products in the versions made available to us were more of the nature of toys than of serious security measures. If it does not want to gamble away the trust in biometric technology right from the start, the line of business should not treat the security needs of its customers quite so thoughtlessly.

As long as adequate security cannot be guaranteed through biometric solutions the use of these products should always be coupled when possible with the assigning of additional PINs or passwords: For most of the solutions doing so is a standard option. When capacitive fingerprint scanners are being used the sensors' surfaces should be cleaned after every use to prevent possibly present latent images from being reactivated. Moreover, anyone using biometric access protection procedures in a Windows 98 or Windows ME environment, should immediately block all avenues whereby regular enrollment might be bypassed. (pmz)

top

A Need for Clarification with Regard to Biometric Applications

The government of the Federal Republic of Germany continues to consider biometric procedures important tools in the fields of identity ascertainment and criminal prosecution. This emerges from the answer given on April 24th to the official question posed to the government by the speaker on domestic policy of the parliamentary group of the PDS (the Party of Democratic Socialists, Germany's reformed ex-communists), Ms. Ursula Jelpke. Referring explicitly to the report on biometrics by c't magazine (c't edition 5/02) Ms. Jelpke had sought to determine the attitude of the federal government to the error rates of these recognition systems and the current state of affairs with regard to the possible introduction of biometric data to identity cards.

Responding to the official question, the ministry of the interior declared that no bill on the introduction of biometric features to and storage of the latter upon identity documents would be introduced to parliament until the requisite preliminary work had been completed. As a first step the procedures in question would have to be tested 'in pilot projects of considerable scope that as to their environmental features simulate as closely as possible the actual later environment of use of the applications.' According to the ministry, there is thus no fixed date for the introduction of the bill. The use of biometric procedures with regard to identity documents had, however, already been discussed at a ministerial level within the EU, the ministry's statement continued, and for June 2002 a conference on this topic of all EU member states was planned.

As there are presently at least five totally different biometrics approaches vying for the customers' favor and the scale of a later application at a total of 70 million owners of German ID documents is clearly defined, the testing is likely, from a technical point of view at least, to take up some time yet.

The assessment of the situation by the Office of Technology Assessment (TAB) of Germany's lower chamber of parliament, the bundestag, is similar: 'An assessment of the capabilities of the available biometric systems on the basis of the - at times highly contradictory - items of information regarding them cannot reliably be undertaken,' thus the office summarizing its insights. The confusion were compounded, according to the office, by the unclear distinctions frequently made between the possible potential and the actual current capabilities of the devices and programs. The TAB, founded in 1990, is an institution that, upon a request by the parliamentary committee on research, furnishes the members of parliament with topic-related reports on and analyses of scientific and/or technical developments, whilst supplying them with information on the related options for political action available. To accomplish its tasks it normally relies on the expertise of independent, external experts. *Richard Sietmann*

top

Attacking Via the USB Port

Taking account of security concerns is not a forte of the protocol of the USB, the Universal Serial Bus. It allows users to swap devices hooked up to a computer while the computer is running; thereby, giving potential assailants something of a break: It allows them to exchange the biometric scanner for a deceptive device of their own and play back to the computer data gathered while eavesdropping on a login event.

The simplest eavesdropping tool is a filter driver like USB Snoop for Windows. USB Snoop interposes itself between the driver of the USB adapter and the actual device driver. After being presented by Windows with all the data exchanged between the USB and the device driver, USB Snoop then writes these into a log file of its own. These data the snooping party can then analyze at its leisure. Filter drivers are quite easy to detect though and in addition require administrator rights to be installed under Windows 2000 and Windows XP. Nevertheless, they would permit studies of a biometric scanner of the same kind as the one to be tricked to be undertaken at one's own PC.

On the other hand, the workings of a hardware analyzer like the USB Agent by Hitex (see page 69), which eavesdrops on the USB cable directly, are virtually invisible. A USB Agent latched on to the cable records all transmitted data, transferring these to a foreign PC. An assailant can then with the aid of the software that goes with the device analyze on the foreign PC the protocols used by the target PC and filter out the relevant data packages. After exporting the data to a text file it is then possible to generate within it the data required to accomplish a login.

With the aid of data packets gathered by eavesdropping and some lines of Perl script we were able to reconstruct complete fingerprints.

With regard to the ID Mouse by Siemens we were able with the aid of USB data packets and a few lines of Perl script to reconstruct the image of a fingerprint. All one requires to replay the data gathered by eavesdropping is a micro controller with USB support and some storage capacity. Together these then constitute a device capable of impersonating towards the target PC the previously removed biometric scanner. The firmware required to do so is fairly easy to program: The device, upon configuration requests, simply needs to respond with answers identical to those of the actual scanner and then at the right moment play back the stored biometric data.

The way to foil attacks of this kind with certainty would be to use so-called challenge-response procedures in the course of which the biometric scanner and the application mutually authenticate one another and thereafter communicate with one another exclusively in an encrypted fashion. (hes)

Translated by Robert W. Smith

BIOMETRICAL FINGERPRINT RECOGNITION:
DON'T GET YOUR FINGERS BURNED

AUTHOR(S)	: Ton van der Putte and Jeroen Keuning
EMAIL	: Ton.vanderPutte@AtosOrigin.com and Jeroen.Keuning@AtosOrigin.com
COMPANY	: Atos Origin
DOCUMENT DATE	: 21 September 2000
NUMBER OF PAGES	: 16

This article is published in the proceedings of:
IFIP TC8/WG8.8 *Fourth Working Conference on Smart Card Research and Advanced Applications*, pages 289-303, Kluwer Academic Publishers, 2000.

Contents

1 Abstract

One of the most critical issues to solve when building multi-accessible systems, such as computer applications, cars or physical buildings, is to determine the identity of a person. A system protecting confidential information, or items of value, puts strong security demands on the identification. Biometry provides us with a user-friendly method for this identification and is becoming a competitor for current identification mechanisms, especially for electronic transactions. However, there are ways to compromise a system based on biometric verification. This article focuses on the drawbacks and risks of biometric verification, specifically verification based on fingerprints. It shows how all currently available fingerprint scanners can be fooled by dummies that are created with very limited means and skills.

This article should be read as a warning to those thinking of using new methods of identification without first examining the technical opportunities for compromising the identification mechanism and the associated legal consequences. This is especially true for people working with smart cards since it is quite common to store fingerprints on smart cards and due to the developments in solid state fingerprint scanners, integration of a fingerprint scanner on a smart card is possible.

2 Introduction

Identification systems based on biometrics are capable of identifying persons on the basis of either physical or behavioural characteristics. Currently, there are over ten different techniques available to identify a person based on biometrics. The following techniques are applied within the main categories physical and behavioural characteristics:

Behavioural characteristics	Physical characteristics
keystrokes dynamics	iris recognition
voice recognition	retina recognition
signature dynamics	vein pattern recognition
	face recognition
	recognition of hand or finger geometry
	fingerprint recognition

Before a system is able to verify the specific biometrics of a person, it of course requires something to compare it with. Therefore, a profile or template containing the biometrical properties is stored in the system. Recording the characteristics of a person is called enrolment. In order to get a profile that corresponds most with reality, the biometrical characteristics are scanned several times. In case of fingerprint recognition the finger is scanned three to four times to get a profile that is independent of variations that occur in practice, such as the angle of placement of the finger on the scanner. Since storage capacity for the profiles in these systems is usually limited (for example if used in combination with smart cards), it is common to use data compression before storing the profile. Storing profiles in tokens requires a combination of token and biometry for verification and therefore gives a higher level of security.

When a biometrical verification is to occur, a scan of the biometrics of a person is made and compared with the characteristics that are stored in the profile. In general, a certain margin of error is allowed between the observed and stored characteristics. If this margin is too small, the system will reject a righteous person more often while if this margin is too large, malicious persons will be accepted by the system. The probabilities that a righteous person will be rejected and that a malicious person will be accepted, are called *False Reject Rate* (FRR) and *False Accept Rate* (FAR) respectively. When using a biometric system, one would of course want to minimise both rates, but unfortunately these are not independent. An optimum trade-off between FRR and FAR has to be found with respect to the application.

3 Biometric Identification Based on Fingerprints

In this chapter the techniques for fingerprint identification will be explored. After explaining the theory of fingerprint verification, all current scanning technologies are described in more detail. Once it is known how these scanners identify a person by means of a fingerprint, two methods to counterfeit fingerprints are shown. All additional methods implemented by scanner manufacturers to prevent counterfeits from being successful are also described together with proposed methods how these systems could also be fooled into accepting dummy fingerprints. The consequences for systems using fingerprint verification are discussed at the end of the chapter. First, an example for fingerprint verification from practice will be given. This example also illustrates how difficult it can be to find an optimum trade-off between FAR and FRR. From a security point of view, one would want to have the FAR as small as possible. However, for acceptance of a biometry system, a large FRR is worse.

Case: Within the car industry a biometric verification system is under evaluation. Some manufacturers of expensive cars are considering using fingerprint recognition as a requirement for ignition of the engine. To arm against car theft, the FAR should be as small as possible. On the other hand, suppose that the righteous owner of a car cannot use his car because his fingerprint is rejected (i.e. FRR is too high). He will consider this to be a much more serious flaw in the system than a technical failure which prevents the car from being started. This is especially true if he compares the advantages of this system with this rejection: the advantages are that the driver does not (necessarily) have to have a key to his car and a perception of higher security with respect to theft of his car. Whether indeed the security improves is questionable. Right now, we do not see car thieves trying to copy the key of your car, instead they try to by-pass the ignition mechanism where the car key is involved. Furthermore, as this article will show, it might decrease security since it is fairly easy and cheap to copy a fingerprint from a person, even without the person knowing this.

3.1 Theory of Fingerprint Verification

The skin on the inside of a finger is covered with a pattern of ridges and valleys. Already centuries ago it was studied whether these patterns were different for every individual, and indeed every person is believed to have unique fingerprints [2]. This makes fingerprints suitable for verification of the identity of their owner. Although some fingerprint recognition systems do the comparison on the basis of actual recognition of the pattern, most systems use only specific characteristics in the pattern of ridges. These characteristics are a consequence from the fact that the papillary ridges in the fingerprint pattern are not continuous lines but lines that end, split into forks (called *bifurcation*), or form an island. These special points are called *minutiae* and, although in general a fingerprint contains about a hundred minutiae, the fingerprint area that is scanned by a sensor usually contains about 30 to 40 minutiae [5].

For over hundred years law enforcement agencies all over the world use minutiae to accurately identify persons [2]. For a positive identification that stands in European courts at least 12 minutiae have to be identified in the fingerprint. The choice of 12 minutiae is often referred to as "the 12 point rule" (see also [1]). This 12 point rule is not based on statistical calculations but is empirically defined based on the assumption that, even when a population of tens of millions of persons are considered, no two persons will have 12 coinciding minutiae in their fingerprints (see [3]). Most commercially available fingerprint scanners give a positive match when 8 minutiae are found. Manufacturers claim a FAR of one in a million based on these 8 minutiae, which seems reasonable.

3.2 Fingerprint Scanning Technologies

Technologies for scanning fingerprints have evolved over the past years. The traditional method which is used by law enforcement agencies for over a hundred years now is making a copy of the print that is found at a crime scene or any other location and manually examining it to find minutiae. These minutiae are compared with prints from a database or specific ink prints, which could be taken at a later time. This method is of course based on the fact that the person who left the fingerprints is not co-operating by placing his finger on a fingerprint scanner. For systems that are commercially available (and deployed) people are required to co-operate in order to gain access to whatever is protected by the verification system.

The first generation fingerprint scanners appeared on the market in the mid eighties, so the technology is about fifteen years old. Over the past few years the technology for scanning fingerprints for commercial purposes has evolved a lot. While the first generation sensors used optical techniques to scan the finger, current generation sensors are based on a variety of techniques. The following techniques are deployed in commercial products that are currently available:

- Optical sensors with CCD or CMOS cameras
- Ultrasonic sensors
- Solid state electric field sensors
- Solid state capacitive sensors
- Solid state temperature sensors

The techniques will be described in greater detail in this section. The solid state sensors are so small that they can be built into virtually any machine. Currently a sensor is in development that will be built in a plastic card the size of a credit card, not only with respect to length and width but also with respect to thickness! It is clear that this type of sensor will give a boost to the number of applications using fingerprint technology.

Optical Sensors

With optical sensors, the finger is placed or pushed on a plate and illuminated by a LED light source. Through a prism and a system of lenses, the image is projected on a camera. This can be either a CCD camera or, its modern successor, a CMOS camera. Using frame grabber techniques, the image is stored and ready for analysis.

Ultrasonic Sensors
Ultrasonic techniques were discovered when it was noticed that there is a difference in acoustic impedance of the skin (the ridges in a fingerprint) and air (in the valleys of a fingerprint). The sensors that are used in these systems are not new, they were already being deployed for many years in the medical world for making echo's. The frequency range, which these sensors use, is from 20kHz to several GigaHertz. The top frequencies are necessary to be able to make a scan of the fingerprint with a resolution of about 500 dots per inch (dpi). This resolution is required to make recognition of minutiae possible.

Electric Field Sensors
This solid state sensor has the size of a stamp. It creates an electric field with which an array of pixels can measure variations in the electric field, caused by the ridges and valleys in the fingerprint. According to the manufacturer the variations are detected in the conductive layer of the skin, beneath the skin surface or *epidermis*.

Capacitive Sensors
Capacitive sensors are, just as the electric field sensors, the size of a stamp. When a finger is placed on the sensor an array of pixels measures the variation in capacity between the valleys and the ridges in the fingerprint. This method is possible since there is a difference between skin-sensor and air-sensor contact in terms of capacitive values.

Temperature Sensors
Sensors that measure the temperature of a fingerprint can be smaller than the size of a finger. Although either width or height should exceed the size of the finger, the other dimension can be fairly small since a temperature scan can be obtained by sweeping the finger over the sensor. The sensor contains an array of temperature measurement pixels which make a distinction between the temperature of the skin (the ridges) and the temperature of the air (in the valleys).

3.3 Counterfeiting Fingerprints

The biggest problem when using biometrical identification on the basis of fingerprints is the fact that, to the knowledge of the authors, none of the fingerprint scanners that are currently available can distinguish between a finger and a well-created dummy. Note that this is contrary to what some of the producers of these scanners claim in their documentation. We will prove the statement by accurately describing two methods to create dummies that will be accepted by the scanners as true fingerprints. The two methods vary based on the co-operation of the fingerprint owner. Although there will without doubt be more ways to counterfeit fingerprints, the methods described in this article should suffice to show that all current scanners can be fooled. Results of tests of current scanners can be found in Appendix C.

Duplication With Co-operation
Duplication of a fingerprint with co-operation of its owner is of course the easiest method since it is possible to compare the dummy with the original fingerprint on all aspects and adapt it accordingly. First, a plaster cast of the finger is created. This cast is then filled with

silicon rubber to create a wafer-thin silicon dummy (see also Figure 1). This dummy can be glued to anyone's finger without it being noticeable to the eye. For a thorough description of how to create such a dummy, we refer to Appendix A which describes the materials and tools that can be used. From the appendix it follows that creation of this type of dummy is possible with very limited means within a few hours.

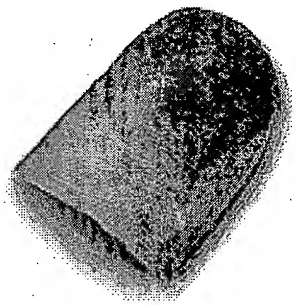


Figure 1: A wafer-thin silicon dummy of a fingerprint

Duplication Without Co-operation

For duplication of a fingerprint without co-operation of its owner it is necessary to obtain a print of the finger from for example a glass or another surface. One of the best ways to obtain such a print could be the fingerprint scanner itself. If the scanner is cleaned before a person will be using it, an almost perfect print is left on the scanner surface since people tend to press their finger (which is the verification finger!) firmly on the scanner. Some more expertise is required to create a dummy from such a print, but every dental technician has the skills and equipment to create one. An accurate description of how to create a dummy of the fingerprint can be found in Appendix B. A picture of a stamp that is created using this method can be found in Figure 2.

Figure 2: A stamp type dummy of a fingerprint

3.4 Additional Tests of Scanners

The main problem that challenges scanner manufacturers is making a distinction between dummy material that is not alive (i.e. silicone rubber) and material that is in fact not alive as well, the epidermis of a finger. Much research is done to make sure that a living finger is behind the epidermis. This research focuses on properties such as temperature, conductivity, heartbeat, blood pressure etc.. Although the methods are able to distinguish between dummies and real fingers, their operation margins have to be adjusted so radically to effectively operate indoors, outdoors, summer and winter, that a wafer-thin silicone rubber that is glued to a real finger easily passes these additional tests of scanners. For each of the possible additional tests for living fingers, a description will be given how dummies can be accepted by these systems.

Temperature

In a normal environment the temperature of the epidermis is about 8-10 degrees Celsius above the room temperature (18-20 degrees Celsius). By using the silicone rubber as described in Appendix A, the temperature transfer to the sensor decreases by at most 2 degrees if compared to a regular finger. It is clear that the difference falls with normal margins that are used on this system (at least 26-30 degrees). Sensors that are also capable of working outdoors are set to accept finger temperatures in an even broader range. Even when these sensors are compensating the fact that they are used outdoors, wafer-thin silicone rubbers won't be detected.

Conductivity

With most fingerprint scanners it is possible to add sensors which measure the conductivity of the finger. The conductivity of a regular finger is dependent on the type of skin (normal or dry). A normal conductivity value is about 200k Ohm (also dependent on the type of sensor), but the same finger will have a conductivity of several mega-Ohms during dry freezing winter weather and only several kilo-Ohms during summer when it is sweaty. Taking this into account, it is obvious that the margins are so large that putting some saliva on the silicone dummy will fool the scanners into believing it is a real finger.

Heartbeat

Several scanner manufacturers claim to detect a living finger by detecting the heartbeat in the tip of the finger. This is very well possible, although some practical problems arise from this. People actively participating in a sport can have heart rhythm of less than forty beats per minute, meaning that they should keep their finger motionless on the sensor for at least four seconds for the rhythm to be detectable. Also, the diversity in heart rhythm of a single person makes it virtually impossible to use it to take a person's heart rhythm into account when scanning the fingerprint. For example, the next day the same sportsman can have a heart rhythm of eighty beats per minute (doubled) if he decides to take the stairs instead of the elevator, just before his fingerprint is scanned. Moreover, the heartbeat of the underlying finger will be detected and accepted when a wafer-thin silicone rubber is used.

Relative Dielectric Constant

The dielectric constant of a specific material reflects the extent to which it concentrates the electrostatic lines of flux. Some manufacturers use the fact that the Relative Dielectric Constant (RDC) of human skin is different from the RDC of, for example, silicone rubber. Just as with conductivity measurement in fingerprint scanners, the RDC is influenced by the humidity of the finger. To prevent an unacceptably high FRR, the margin of operation should be rather large. Putting some spirit on the silicone rubber with a wad of cotton wool before it is pressed on the fingerprint scanner fools the additional dielectric sensor. Spirit consists of 90\% alcohol and 10\% water. The RDCs of alcohol and water are 24 and 80 respectively, while the RDC of a normal finger is somewhere between these two values. Since the alcohol in the spirit will evaporate quicker than the water, the rate alcohol/water in the evaporating spirit will go to 0 (i.e. spirit slowly turns into water). During evaporation the RDC of the dummy will go up until it falls within the margins of the scanner and will be accepted as a real finger.

Blood Pressure

There are sensors available with which the blood pressure can be measured by using two different places on the body. They require a measurement of the heartbeat on two different places to determine the propagation speed of the heart pulse through the veins. Apart from the disadvantages that were already mentioned with the heartbeat sensors, this technique has an additional disadvantage in requiring measurement on two different places, i.e. on two hands. Similar to the heartbeat sensors, this method is not susceptible to a wafer-thin silicone rubber glued to a finger. Single point sensors are available but they must be entered directly in a vein, which obviously makes them unusable as a biometric sensor.

Detection Under Epidermis

Some systems focus on detection of the pattern of lines underneath the epidermis. The pattern of lines on this layer is identical to the pattern of lines in the fingerprint. Although this type of sensors look underneath the first layer doesn't mean that they cannot be fooled by dummy fingers, once it is known how they distinguish between the epidermis and the underlying layer.

Some methods use the fact that the underlying layer is softer and more flexible than the epidermis (ultrasonic sensors could use this), while others focus on the higher electric conductivity of the underlying layer. Once it's known which property the sensor uses, a second silicone rubber with matching properties can be created. It is more difficult to create a dummy that is wafer-thin as described in Appendix A, but for a dummy as described in Appendix B it is rather easy. First, a conductive, soft or more flexible rubber print is made which can be used as the basis to which the regular silicone rubber is attached. Making sure that the two line patterns are in exact matching positions is no problem for a dental technician.

Other Claims
Some manufacturers claim to use even more exotic detection methods and techniques than the ones described above, making claims to having built a sensor which is not even known or being used in medical science. Additionally, they refuse to reveal the detection method claiming it is a company secret. Claims by these manufacturers should, without a doubt, be considered nonsense! In general, *security by obscurity* (trust that, by keeping specifications secret, the system will not be broken) should never be used. Although obscurity can make it more difficult for people to break the system in a brief period after introduction, most systems can be reverse engineered or worked around in ways the designers never expected.

3.5 Consequences of Counterfeit Possibilities

The possibility to make a dummy, which will be accepted by the fingerprint scanners, makes the system weak with respect to some different attacks:

1. A malicious person who wants to gain access, inconspicuously intercepts a fingerprint from someone who is granted access. With this print, a dummy is created.
2. If a righteous person is willing to co-operate, one or several dummies can be created with which this individual can give access to whomever he wishes.
3. If a righteous person handles a transaction, he can claim to be framed by a malicious person as described in point 1.

While the first two attacks on the system are possible with most verification systems, the third claim can usually be disproved since the person making the claim must have revealed something. An example is fraud with a PIN protected credit card. If the fraud is committed using the PIN code, the probability that its owner has not been careful with the PIN is much higher than the probability that the PIN system is broken. But the fingerprint verification system is very susceptible to this attack since we all leave behind fingerprints everyday, everywhere without noticing it. As long as it is still possible to use either the methods from this article, or other methods to work around a fingerprint verification system, deployment of such systems is unsuitable for virtually any application.

Case:
Suppose that a bank decides that for transactions, which exceed a certain amount of money, identification of the employee performing the transaction is required. The argumentation to use fingerprint verification instead of for example username/password combinations are that in case of fingerprint verification, the employee has to be present and cannot transfer his username/password to a colleague to perform transactions for him. Other systems that are considered, such as smart cards, can also not prevent the employee from letting other people perform a transaction. The bank trusts on the solution presented to them and decides to roll-out the fingerprint verification system throughout all offices.

An employee of the bank knows that these systems can be circumvented and decides to make a dummy from a fingerprint of a colleague. The risks are small since using the fingerprint of a colleague cannot be traced back to him. To obtain the fingerprint he asks the colleague who's fingerprint he intents to use to hand him a glass or plate. This will almost

certainly leave a perfect print on a clean surface, with which a dummy can be created and the fraudulent transactions can be performed. In case the malicious employee is not capable of creating a good dummy, he can always perform transactions using his own finger and claim that he is framed by a colleague the same way as described above.

4 Conclusion

Manufacturers of fingerprint scanners currently cannot deliver convincing evidence that they can make a distinction between a real, living finger and a dummy created from silicone rubber or any other material. Therefore, our advice is not to use fingerprint verification with applications where the identification serves as proof of presence. Comparing all biometric verification possibilities, fingerprint scanners are (perhaps apart from keystroke dynamics) the least secure means of verification. It is the only system where the biometrical characteristic can be stolen without the owner noticing it or reasonably being able to prevent it.

Even in a case where confidential computer data are protected by means of fingerprint verification we advise use of this verification only in combination with a token, for example a smart card, on which the user's template is stored. This prevents unnoticed access by someone using a dummy when the template, with which the scanned finger is compared, is stored on the computer's hard disk. The security level of the combination of fingerprint verification and smart card should be compared to username/password security. The former can be considered more user-friendly.

With all applications that are considered to be protected by using biometric verification, techniques to compromise the system such as described in the appendices of this article should be very thoroughly examined. It should of course be taken into account that someone can break into a system if they put enough effort and resources into it (which is of course common with security issues). A problem with fingerprints is that neither the resources nor the skills to create a dummy are uncommon. Furthermore, the possibility of someone claiming to have been framed by someone else using methods that could not reasonably be prevented, must be eliminated. Otherwise the system is not suitable for the application.

5 Disclaimer

This article is based on private material and information that was released by fingerprint scanner manufacturers (also [4]). Many of the statements in this article are based on technology that is currently available. New technologies may evolve to a full fingerprint scanner between the submission deadline of this article and the actual CARDIS conference. These results or proof from fingerprint manufacturers that they can actually make a distinction between living fingers and well created dummies will of course be discussed at the conference.

Appendix A - Duplication With Co-operation

This appendix describes, step by step, how to create a wafer-thin silicon dummy of a fingerprint if the owner of the fingerprint is willing to co-operate. The method requires only a limited amount of time (a few hours) and limited means (only cheap and easy accessible materials are used).

1. Beforehand, the finger should be washed with soap to make plaster flow more easily through the valleys of the print.
2. Using modelling-wax a kind of saucer or bowl is formed at the nail side of the finger and around the tip of the finger (like a thimble with an opening where the actual fingerprint is). This bowl is filled with plaster to obtain a print of the finger. Preferably the plaster should be of a good quality (such as used by dental technicians or kits for creating plaster figures sold in hobby shops).
3. The dried plaster is a bowl with a perfect fingerprint inside. In order to make a very thin dummy, a pounder that fits the mould (apart from a 1 mm distance for the dummy) can be created using plaster.
4. Silicon waterproof cement (available in any do-it-yourself shop) or liquid silicon rubber is placed in the mould and the pounder is pressed firmly on top of this layer.
5. When the silicon has hardened, the dummy should be very carefully removed and is ready.

Appendix B - Duplication Without Co-operation

In order to make a dummy from a fingerprint without co-operation of its owner, a remake of a fingerprint that was left behind somewhere has to be made. The resulting dummy can of course be no better than the print itself so that for a good dummy a good print is required.

1. First the print has to be copied from the material it is left on. The method used by the police can very easily be used for this. Visualisation of the print is done with a very fine powder put on the print with a brush. Some scotch tape is used to remove the powder from the underground.
2. A camera and film are used to create a photo of the print by placing the tape on the photosensitive side of the film and making a picture of a diffuse light source.
3. After developing the film, the negative is attached to a photosensitive PCB. This is exposed to UV light after which the negative is removed and the PCB will be developed. Using an etching bath, the parts of the PCB that were exposed to the UV light are washed away. A final etching bath (sour) etches the copper layer. The result is a very slim profile (about 35 micron) that is an exact copy of print, copied in step 1.
4. After deepening (with for example a Dremel) the profile to resemble the depth of a regular fingerprint, a silicon waterproof cement stamp can be created.

This method creates an almost perfect copy of the finger in about eight hours, using materials that are available in do-it-yourself shops and electronics shops. It requires more

skills to create this dummy than the one described in Appendix A, but again, any dental technician or handyman has the necessary skills.

Appendix C - Tested Fingerprint Sensors

Since 1990 several fingerprint sensors have been tested using dummy fingers, as described in this article. All tested sensors accepted a dummy finger as a real finger, almost all at the first attempt. The following table shows the tested scanners, the date on which it has been tested and the number of attempts required to get a dummy finger accepted.

Manufacturer	Model	Technology	Date	Difficulty
Identix	TS-520	Optical	Nov. 1990	First attempt
Fingermatrix	Chekone	Optical	Mar. 1994	Second attempt
Dermalog	DemalogKey	Optical	Feb. 1996	First attempt
STMicroelectronics	TouchChip	Solid state	Mar. 1999	First attempt
Veridicon	FPS110	Solid state	Sept. 1999	First attempt
Identicator	DFR200	Optical	Oct. 1999	First attempt

In the period 1994 till 1998, more optical sensors have been tested on various fairs (mainly the CeBIT fair in Hannover, Germany). All sensors accepted the silicone dummy finger at the first attempt. The tested sensors are not listed in the table since no thorough list of manufacturers and models has been made at that time.

6 Bibliography

[1] Kingston, C.R. and P.L. Kirk, ``*Historical Development and Evaluation of the `12 Point Rule' in Fingerprint Identification,*'' International Criminal Police Review, 1965.

[2] Lee, H.C. and R.E. Gaesslen, *"Advances in Fingerprint Technology,"* Elsevier, New York, 1991.

[3] Zeelenberg, A.J., ``*Het identificatieproces van dactyloscopische sporen,*'' VUGA, 's-Gravenhage, 1993 (in Dutch).

[4] http://www.biometrics.org

[5] http://www.infineon.org

BIOMETRICS AND YOUR PRIVACY

What's All the Fuss About?

The Electronic Privacy Information Center's Biometric Privacy page (see Links) points out six major areas of concern regarding the use of automated biometric devices: "Biometric identifiers are of course widely used by people to identify each other – one might recognize a friend by the sound of her voice, the color of her eyes, or the shape of her face. Devices using biometric identifiers attempt to automate this process by comparing the information scanned in real time against an "authentic" sample stored digitally in a database. The technology has had several teething problems, but now appears poised to become a common feature in the technological landscape. There are significant privacy and civil liberties concerns regarding the use of such devices that must be addressed before any widespread deployment. Briefly there are six major areas of concern:

1. Storage. How is the data stored, centrally or dispersed? How should scanned data be retained?
2. Vulnerability. How vulnerable is the data to theft or abuse?
3. Confidence. How much of an error factor in the technology's authentication process is acceptable? What are the implications of false positives and false negatives created by a machine?
4. Authenticity. What constitutes authentic information? Can that information be tampered with?
5. Linking. Will the data gained from scanning be linked with other information about spending habits, etc.? What limits should be placed on the private use (as contrasted to government use) of such technology?
6. Ubiquity. What are the implications of having an electronic trail of our every movement if cameras and other devices become commonplace, used on every street corner and on every means of transportation?"

Other experts' concerns and the BioPrivacy Initiative's Impact Framework (see Resources page) align very closely with the above. There are also some promising proposed solutions that we will examine. These solutions seem to be receiving much less press than the "Big Brother" problems. Let's examine these concerns and how they may affect you personally.

Identification, Verification and Databases

Identification matches a physiological or behavioral characteristic of a person to a pre-confirmed record of that characteristic. For example, matching the image of my face to a photograph in a large number of photos in a database, or comparing a "new or candidate" fingerprint to many sets of fingerprints in an existing database. These "one-to-many" (1:N) search techniques compare a sample with data in a database and are at the core of the identification process.
In contrast is a "one-to-one" (1:1) search, used when we are accessing such things as our bank machine. Verification is done through the presentation of a "token" such as a PIN, a card, or a biometric whose validity is confirmed, and thereby verifying one's eligibility to access a particular service. There is no searching and matching to a database, only the validity of the token is established, through a single one-to-one match.

Databases are at the root of EPIC's privacy concerns #1, 2, and 4 above. Concerns about storage, vulnerability, and authenticity are very real. The biometric database is the ultimate target for all sorts of mischief from within and without the organization that owns it. Database oriented solutions also cause a very practical operational limit because you need access to the (highly protected) database every time you wish to identify someone or verify a token. This all leads towards expensive solutions.
There are promising alternatives that move the database. One solution (see Resources page) use a "smart" card with your biometric data encrypted on the card. You then must read the smart card, and have a secure system for creating the cards. In this case, key management would be the weak link. In an excellent address to a Privacy and Law Symposium Canadian scientist, Dr. George Tomko (worth reading, see Resources page), argues that your biometrics **should be** the encryption. To our knowledge this approach has not yet been implemented.

Confidence and Consequences

When the implications of false results are very serious, then the 1:N identification systems are at their worst. Dr. Philip Agre of UCLA points out (see Arguments against Automatic Face Recognition in Public Places on the Resources page) that face recognition is nearly useless for the application that has been most widely discussed since the September 11th attacks on New York and Washington: identifying terrorists in a crowd. The reasons why are statistical – a 99.99 percent accurate system that scans 10 million faces will produce 999 errors for each correct match of a real terrorist. The enormous percentage of false matches will condition security workers to assume that all positive matches are mistaken.
Also, 99.99% accuracy is overly optimistic. According to experts, facial recognition has only about an 85% success rate for matching, while fingerprints range close to 99% accuracy. Spotting terrorists in a crowd is a needle-in-a-haystack problem, and most biometric techniques are not a needle-in-a-haystack-quality technology.

Linking and Ubiquity

In the article cited above, Philip Agre accurately points out: "Many social institutions depend on the difficulty of putting names to faces without human intervention. If people could be identified just from looking in a shop window or eating in a restaurant, it would be a tremendous change in our society's conception of the human person. People would find strangers addressing them by name. Prospective customers walking into a shop could find that their credit reports and other relevant information had already been pulled up and displayed for the sales staff before they even inquire about the goods. Even aside from the privacy invasion that this represents, premature disclosure of this sort of information could affect the customer's bargaining position."
This is a polite example about the dangers of linking information. Other linkages, by both public and private parties, could be far more invasive and destructive.

Good Metrics of Good Biometrics

The International Biometrics Group "BioPrivacy Impact Framework" provides a means of assessing the privacy risks involved in a real or proposed biometric deployment. A private-sector biometric application in which the user retains ownership of his or her biometric information is much less likely to negatively impact user privacy than a covert public identification system; the precautions taken in each

system will be proportional to the potential risks related to the use of that system. Though there are many additional factors to assess, such as the political climate and legal backdrop for biometric usage, the existing Impact Framework provides a starting point for intelligent assessment and categorization of biometric systems. The Impact Framework considers these factors:

1. Overt vs. Covert. Deployments in which users are aware that biometric data is being collected and used, and acquisition devices are in plain view, are less privacy-invasive than surreptitious deployments.
2. Opt-in vs. mandatory. A biometric system in which enrollment is mandated, such as a public sector program or one designed to encompass a company's employees, bears a more direct relationship to privacy risks than an opt-in system.
3. Verification vs. identification. (see above) A system capable of performing 1:N searches can be considered more susceptible to privacy-related abuse than a 1:1 system.
4. Fixed duration vs. indefinite duration. In deployments where such an option exists, the use of biometrics for a fixed duration is less likely to have a negative impact on privacy than one deployed indefinitely.
5. Public vs. private sector. Suitable protections should be developed for each type of environment.
6. Individual, customer, student, traveler, employee, citizen. An individual's roles vary according to the people and institutions with whom they interact. Although privacy rights are fundamental regardless of the institution with whom the person is interacting, they are not identical in all environments. Reasonable expectations of privacy are dependent on the capacity in which a person is interacting with another person or institution: anonymous individual, customer, student, traveler, citizen, employee, prisoner.
7. User ownership of biometric data vs. institutional ownership. Deployments in which the user maintains ownership over his or her biometric information are more likely to by privacy-sympathetic than those in which the public or private institution owns the data.
8. Personal storage vs. template database. A biometric system which stores information centrally is clearly more capable of being abused than one in which biometric information is stored on a user's PC or even on a smart card.
9. Behavioral vs. physiological biometric. Behavioral biometrics are much less likely to be deployed in a privacy-invasive fashion, as technologies such as voice-scan and signature-scan can be easily changed by altering a signature or using a new pass phrase. Physiological biometrics are much harder to mask or alter, and can be collected without user compliance.
10. Give vs. grab biometric information. Biometric systems in which data capture is initiated by the user are less likely to be deployed in a privacy-invasive fashion than those which automatically capture data. The "give" systems require explicit user consent to capture data, while the "grab" systems can capture data without the user's explicit approval.

Good News Too - A Banking Example

Regulators require that bank employees be fingerprinted. The traditional process for processing fingerprints requires twelve weeks to determine if an employee is fit to work in the bank. Bankers have estimated that the processing delay alone costs $3-8 million per year for **each** large commercial bank in the U.S. A newer technology (see Validex Corp. on the Resources page) scans fingerprints on-site, produces results in 24 hours, and cuts losses.

Conclusion

Because they are so important for business and government, you should expect increasing use of biometric techniques in the coming decade. Technologies and policies will both refine. You'll want to remain aware of the issues and knowledgeable enough to make informed choices.

Despite the initial unfavorable publicity surrounding biometric techniques, their use can bring both good and evil. Biometrics could be a simple security improvement over those dozen or two passwords/PINs in your life that are not unique, that you don't really have memorized, and that are possibly written down somewhere.

We will need to learn to deal with this new challenge / opportunity in our public and private lives.

Face-Recognition Technology Improves

- From: R. A. Hettinga
- Subject: Face-Recognition Technology Improves
- Date: Fri, 14 Mar 2003 16:54:44 -0800

<http://www.nytimes.com/2003/03/14/technology/14FACE.html?th=&pagewanted=print&position=top>

The New York Times

March 14, 2003

Face-Recognition Technology Improves
By BARNABY J. FEDER

Facial recognition technology has improved substantially since 2000, according to results released yesterday of a benchmark test by four federal government agencies involving systems from 10 companies.

The data, which is the latest in a series of biannual tests overseen by the National Institute of Standards and Technology, is expected to encourage government security officers to deploy facial recognition systems in combination with fingerprinting and other biometric systems for applications like verifying that people are who they claim to be and identifying unknown people by comparing them with a database of images.

But the report also highlighted continuing shortcomings, like the poor performance of recognition systems in outdoors settings in which even the best systems made correct matches to the database of images just 50 percent of the time. And it cited outcomes that it said needed more research, like the tendency of the systems to identify men better than women and older subjects better than young ones.

The report was strictly a technical evaluation and did not discuss any of the privacy or civil rights concerns that have stirred opposition to the technology.

Because the results of the different companies are public, the testing is also expected to become a marketing tool for those who did best, including Identix, Cognitec Systems and Eyematic Interfaces. It is expected to be especially helpful to Cognitec, a tiny German company that is not widely known in the United States, and Eyematic, a San Francisco-based company best known for capturing data from traits like facial structures, expressions and gait to create animated entertainment.

``Face recognition had been just a subdiscipline for us,'' said Hartmut Neven, chief technical officer and a founder of Eyematic. He said that domestic security needs had created a marketing opportunity that Eyematic was gearing up to chase.

The results were not as positive for Viisage Technology, which had been among the leaders in 2000. Viisage said that the results, that it identified just 64 percent of the test subjects from a database of 37,437 individuals, were at odds with the strong performance it had been having with big customers, like the State of Illinois. While the government test is the largest for such technology, the number of images in the database was far below the 13 million that Viisage deals with for the Illinois

Department of Motor Vehicles, where the company says it has picked thousand of individuals seeking multiple licenses under different names.

``We suspect there must have been human or software errors in how our system was interfaced with the test,'' said James Ebzery, senior vice president for sales and marketing for Viisage. While Viisage scrambles to explain its views to customers and chase down any potential problems in the test, it is taking comfort in the tendency of big companies and government agencies to perform their own testing on their own data before selecting Viisage or one of its rivals.

The government's benchmarking was performed last summer but the results were not fully tabulated and analyzed until recently. The report singled out a finding that in ``reasonable controlled indoor lighting,'' the best facial recognition systems can correctly verify that a person in a photograph or video image is the same person whose picture is stored in a database 90 percent of the time. In addition, only one subject in 100 is falsely linked to an image in the data base in the top systems.

The report also noted that performance has been enhanced by improving technology to rotate images taken at an angle so that the facial recognition software can be applied to a representation of a frontal view.

The data examined whether facial recognition systems could help with the so-called watch list challenge, which involves determining if the person photographed is on a list of individuals who are wanted for some reason and then identifying who they are. Cognitec, the leading performer on that test, gained a 77 percent rating but its success rate fell to 56 percent when the watch list grew to 3,000.

--

R. A. Hettinga <mailto: >
The Internet Bearer Underwriting Corporation <http://www.ibuc.com/>
44 Farquhar Street, Boston, MA 02131 USA
"... however it may deserve respect for its usefulness and antiquity,
[predicting the end of the world] has not been found agreeable to
experience." -- Edward Gibbon, 'Decline and Fall of the Roman Empire'

The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to

- **Face-Recognition Technology Improves**, *R. A. Hettinga*
  - Re: Face-Recognition Technology Improves, *Sidney Markowitz*
    - Re: Face-Recognition Technology Improves, *Derek Atkins*
      - Re: Face-Recognition Technology Improves, *Sidney Markowitz*
      - Re: Face-Recognition Technology Improves, *Bill Stewart*
        - Re: Face-Recognition Technology Improves, *Derek Atkins*
        - Re: Face-Recognition Technology Improves, *Eugen Leitl*
          - Re: Face-Recognition Technology Improves, *Bill Stewart*
            - Re: Face-Recognition Technology Improves, *Eugen Leitl*
            - Re: Face-Recognition Technology Improves, *bear*
          - Re: Face-Recognition Technology Improves, *bear*

<-- Chronological --> <-- Thread -->

Reply via email to
R. A. Hettinga

Can face recognition keep airports safe?

Last modified: November 1, 2001, 5:00 PM PST

By Stefanie Olsen and Robert Lemos
Staff Writer

As U.S. airports begin installing face-recognition systems to thwart terrorism in the wake of the Sept. 11 attacks, civil rights activists are rushing to decry the technology as ineffective and invasive.

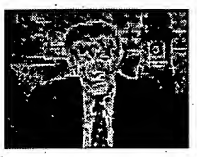
The American Civil Liberties Union on Thursday derided the use of face-recognition software in airports, saying it doesn't work and "offers us neither order nor liberty."

The report comes the same day that ADT Security Services, one of the largest security companies, with a growing presence in airports, agreed to use face-recognition systems from Visionics. Boston's Logan International Airport also announced plans earlier this week to install such technology.

Officials at airports across the country are clamoring to implement additional safety measures to protect travelers and employees against potential terrorist threats. Some security experts, who believe better high-tech surveillance systems could have prevented the Sept. 11 attacks, have said they are optimistic about the use of face-recognition technology and other so-called biometric security devices. But civil rights advocates worry that out-of-date photos and poor lighting could result in numerous misidentifications.

"It is abundantly clear that the security benefits of (face-recognition surveillance) would be minimal to nonexistent, for a very simple reason: The technology doesn't work," according to a report from the ACLU, citing a survey from the Department of Defense on the technology's high margin of error in pinpointing terrorists.

Equally concerned with the technology's rising adoption, high-profile privacy expert Richard Smith abandoned his post at the Privacy Foundation this week to evaluate and consult on security issues surrounding biometrics, including face-scanning devices.



Facing new security at airports
Thomas Colatosti, CEO, Visage Technology

Biometrics is the digital analysis using cameras or scanners of biological characteristics such as facial structure, fingerprints and iris patterns to match profiles to databases of people such as suspected terrorists. Some experts say face recognition is perhaps the most promising biometric technique for overcrowded airports because it relies on distant cameras to identify people--not finger scanners or other devices requiring people to click, touch or stand in a particular position.

Several airports are adopting such face-recognition software in an effort to beef up security after the suicide bombings on the World Trade Center and the Pentagon. In addition to the Logan airport in Boston, Oakland International Airport in Oakland, Calif.;

Top picks from News.com readers

Readers who read **Can face recognition keep airports safe?** also read....

- Biometrics may scan air travelers
- Airport security technology under scrutiny

T.F. Green Airport in Providence, R.I.; and Fresno Yosemite International Airport in California are among those adopting identification technology to check passengers.

As a result, leading biometric companies including Littleton, Mass.-based Viisage Technology and Minnetonka, Minn.-based Visionics are experiencing enormous demand from the government, security officials and investors. Share prices of many of these companies have surged more than 300 percent since Sept. 11.

Visionics, one of the biggest makers of face-recognition systems, signed a deal Thursday with conglomerate Tyco International to distribute Visionics' FaceIt technology through Tyco's ADT unit. ADT provides security systems at some 100 of the nation's 450 commercial airports, ranging from card-entry systems to metal detectors and security cameras.

False sense of security

But civil libertarians say biometric companies are preying on the country's fears about safety rather than offering a promising solution to prevent terrorism.

"Anyone who claims that facial-recognition technology is an effective law-enforcement tool is probably working for one of the companies trying to sell it to the government," according to the ACLU's report.

The group cited a study by the Department of Defense that recorded a high rate of error when identifying suspects--even under ideal settings such as scanning a person's image under bright lights, face forward. The study showed a large number of "false positives," wrongly matching people with photos of others, and "false negatives," missing people not in the database.

NEWS.COMMENTARY

Gartner analyst Bill Keller says that after the Sept. 11 attacks, the United States started to explore the wider use of face recognition technology as an anti-terrorist tool. But this technology has other potential applications that may actually help to preserve privacy and confidentiality.

see commentary

"Facial-recognition software is easily tripped up by changes in hairstyle or facial hair, by aging, weight gain or loss, and by simple disguises," the ACLU report said. "That suggests, if installed in airports, these systems would miss a high proportion of suspects included in the photo database, and flag huge numbers of innocent people--thereby lessening vigilance, wasting precious manpower resources, and creating a false sense of security."

Takeo Kanade, a professor of computer science and robotics at Carnegie Mellon University, agreed--to an extent--with the ACLU's evaluation of facial recognition.

"When it comes to a problem of comparing mug shots from the front under good lighting conditions, and pictures that don't include aging effects, then the problem is a relatively easy problem to solve," he said. Solutions could include placing cameras so they scan people standing in place, such as at a check-in counter metal detector.

"However, the difficulty is recognizing people under varying conditions, (which) is required for a surveillance type of purpose," Kanade added. If the picture is taken from the side, if the person has an animated expression, or even if a person is wearing sunglasses, all can make recognition more difficult.

Yet, Kanade said he believed face recognition could make it easier to ensure airport security.

"The system can be used as a screening method," he said. "If the police have to look at 10,000 people rather than 1 million people, then it is worth it."

Joseph Atick, Visionics' founder and CEO, said in an earlier interview that the technology is best thought of as a first line of defense.

"It gives you somewhere in the 90s (percentile) in terms of effectiveness of the shield.

- Privacy vs. safety
- A database of faces: Pros and cons
- Comdex: Biometrics meets security

Mo

Latest headlines

- Riemann hypothesis may have been solved
- IE flaws used to spread pop-up toolbar
- Bush administration won't appeal phone decision
- Oracle offer holds risks for early takers
- Intel targets China's online gamers
- U.S. broadband access leaped 42 percent in 2003
- Encryption firm says secrets for sale at auction
- EarthLink launches high-speed broadband service
- Briefly: Germany approves Symbian deal
- Germany approves Symbian deal
- TiVo steps into online content
- Security specialist to add Web-filtering tools
- Domain name registration again in vogue
- Ask Jeeves taps into desktop search
- Low-end Power Macs get dual processors

Most popular headlines

- Is the dust on your computer toxic?
- Why the FCC should die
- Yahoo tests new home page
- Microsoft checks off patent win
- Beatles catalog headed for digital distribution?
- Special coverage: Oracle vs. PeopleSoft
- Sony revs up speedy DVD burner
- Apple's AirPort adds home music streaming
- Intel eyeing storage white boxes?
- Linksys Wi-Fi router vulnerability discovered

Without creating any barricades, we can stop nine out of 10 terrorists," he said, adding an oft-quoted axiom in security circles: "There is no such thing as a 100 percent shield."

Visionics' technology can scan about 15 faces a second, compiling 84 bytes of data for each face detected in a frame of video. It maps the landmarks of the face including nose, eyes and mouth to create a digital "faceprint" of a person. The faceprint is then compared to a database of tens of thousands of other biometric IDs representing criminals, terrorists or other people for whom security is looking.

Chasing the wrong people

Atick acknowledged, though, that an average of a handful of false alarms a day, per airport, is likely. If passengers are frequently mistaken for terrorists, it could become a burden for travelers.

In addition, U.S. authorities in many cases don't know who the terrorists are, much less have a picture on file, said security consultant Smith.

"There's kind of a disconnect here," he said. "We can only spot terrorists who we have photos of--and why wouldn't we arrest them sooner in that case? How do we find them if we don't know what they look like?"

The Sept. 11 attacks underscored the United States' limited knowledge about who the terrorists are. Of the 19 Muslim extremists who hijacked the four commercial airlines, only two were reported to be on a CIA watch list.

In the end, the systems may be used far more often for nabbing smaller fish, Smith said.

"What really happens is that we end up going after petty criminals," he said. "A better approach is installing better doors in airplanes so that terrorists can't get in cockpits, which the government is doing."

In its report, the ACLU said that several government agencies including the Immigration and Naturalization Service office have abandoned face-recognition systems after finding they did not work as advertised. The INS, it said, experimented with using the technology to identify people in cars at the Mexico-U.S. border.

Nevertheless, other biometric devices have already made inroads in the United States. For example, New York's JFK airport uses hand scanners, but the purpose is to speed frequent flyers through customs--not to spot terrorists.

The Department of Defense has also funded the development of face-recognition technology as a weapon in its war on drugs. Department officials tested the technology to increase border security several years ago with "varying success." It continues to evaluate the effectiveness of the technology today.

"Face recognition at this time is still a very new technology. As with any new technology, there are items that have an impact on system effectiveness, including lighting, pose, temporal variation, distance and subject participation," said Stacia Courtney, spokeswoman for the department's Counter Drug Development Program Office.

Iain Drummond, CEO of biometric company Imagys, said that despite concerns, the public will eventually accept face-scanning devices as the norm in airports. Imagys is providing face-recognition software to Oakland International Airport.

"If you look back about 20 years, there were no X-ray machines," he said. "But no one grumbles about it today."

News.com's Rachel Konrad contributed to this report.

YOUR TAKE *What do you think about this story? Tell us now.*

Track this story's companies and topics

Create your own e-mail alert >

Related stories

Privacy expert resigns to focus on security
October 31, 2001

Privacy vs. safety
September 17, 2001

Airport security technology under scrutiny
September 12, 2001

Biometric technology aims to speed air travel
August 2, 2001

Get this story's "Big Picture" >

Related quotes

Quotes delayed 20+ minutes

▼	VISG	9.66	-0.14	(-1.43%)	Viisage Technology Inc
☐	VSNX	8.32	0.00	(0.00%)	0

More quotes >

Physical Security: A Biometric Approach

Ryan Hay
SANS - GSEC Practical
Track 1C
November 12, 2003

Abstract

In the competitive business world today, the negative publicity and financial ramifications from an IT physical security breakage can be disastrous. An IT physical security breakage could and most likely lead to the selling of shares from stockholders, financial revenue and profit loss, numerous corporate lawsuits, disgruntled employees, corporate and brand embarrassment, and exhaustive time and effort spent on problem research and prevention.

When coupled with constant September 11 terrorism concerns and the importance of corporate data privacy, the need and demand for a biometric physical security solution has never been higher. This paper will address biometrics and its history, discuss and analyze various biometric techniques and products, provide advantages and disadvantages of these techniques, and conclude with a discussion on biometrics of the future.

What is biometrics?

In a formal sense, biometrics refers to any automatically measurable, robust, and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual. It is the automatic recognition of a person using distinguishing traits. (1)

From the Greek meaning life (bio) and metric (to measure), the term "biometrics" refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics. In reality, biometrics refers to protecting network and physical security through physical and behavioral biometric techniques.

The physical biometric techniques include fingerprinting, hand and finger geometry, facial recognition, iris and retinal scanning, and vascular pattern recognition. While, behavioral biometric techniques include speaker and voice recognition, signature verification, and keystroke dynamics. All of these techniques will be discussed later in the paper.

For simplicity, both biometric techniques are defined and designed for simple and streamlined identification and verification purposes of a person. In short, biometric *identification* involves determining who a person is and biometric *verification* is determining if a person is who they say they are. (2)

A Biometrics History

One of the first known examples of biometrics in practice, and considered the most popular form of biometrics today, was a form of finger printing used in China in the late 14th century. The fingerprinting involved Chinese merchants stamping children's palm prints and footprints on paper with ink to distinguish them from one another.

In the late Eighteenth century, body measurements were considered an alternative biometric technique. The process was designed for identifying convicted criminals of repeat offenses by measuring and recording a criminal's body, head, and limbs whenever arrested. The process was called Bertillonage. Over time the process proved very time consuming and unreliable.

Today, and mostly over the last three decades, physical security and biometrics have exploded in popularity thanks in large part to the computer revolution and the sensitivity of corporate data. Most corporations integrate a combination of physical and behavioral biometric techniques for their data centers. (Individual Biometrics 2002)

Here are some common physical security biometric techniques.

Physical Biometric Techniques

Fingerprinting

As discussed earlier, is the oldest and most popular physical technique used today. Fingerprinting takes an image (either using ink or a digital scan) of a person's fingertips and records its characteristics. The patterns are matched (ink) or encoded (digital) and then compared with other fingerprint records. Although the popularity of ink is still common, digital scanning is preferred.

With digital scanning, a user presses his or her finger gently against a small optical or silicon reader surface where fingerprint information is taken from the digital scan and sent to a database for verification and identification comparison. (Individual Biometrics 2002)

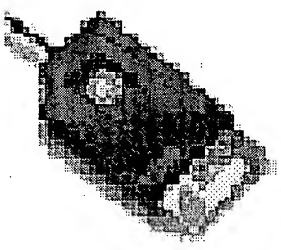


Figure A: IT Security

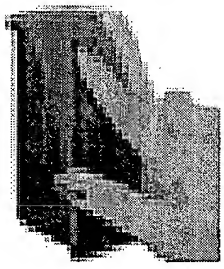


Figure B: Physical Security

Companies like Precise Biometrics of Sweden, are capitalizing on the competitive and dynamic fingerprint market with the development and innovation of IT security (Figure A) and physical access (Figure B) readers. (3)

In short, fingerprint security readers provide for many advantages. Such as a piece of mind in having no passwords or PIN numbers to remember; the elimination of expensive password administration; flexibility and interoperability; an unlimited number of users; preservation of privacy (fingerprint template stored on card); ease of use; and compatibility with all major access control systems. (Precise Biometrics p6)

Conversely, the technology does pose several challenges. Scanner durability form static discharges and vandalism can be seen as a first challenge. High maintenance and cleaning of the scanners is thought of as a second challenge. And, the possibility of tricking the system with fake fingerprints is seen as a final challenge (4)

The future of fingerprinting appears to be very bright, as you will continue to see widespread usage within the law enforcement community and for personal use. Corporations have recently introduced memory stick fingerprint scanners and fingerprint mice to capitalize on the increasing market. Furthermore, a large number of banks will incorporate this as the accepted authorization at ATMs for withdrawing and depositing money and at grocery stores for fingerprint scan checkout and billing to a registered user's credit card or debit account.

Fingerprinting Examples:

Casio Computer and Alps Electric have developed a small fingerprint scanner (Figure C) built into a short, thin cylinder for use in cellular telephones and other portable devices for use in Fall 2003. The cylinder, 0.2 inches in diameter and 0.6 inches long, contains a sensor, light, and lens. When users roll their fingers over the device, it can produce an 8-level monochrome fingerprint image at 600 dots per inch resolution. (5)

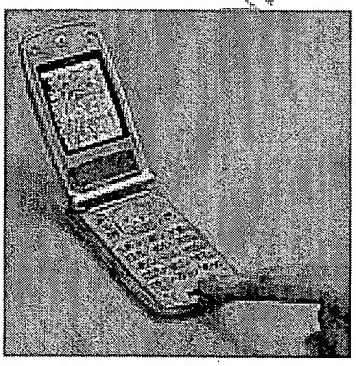


Figure C: Casio Cellular Scanner

Figure D: HP IPAQ H5450

Hewlett-Packard (Figure D) became the first manufacturer to add biometric identity checking to a mass-market consumer portable electronics device last year, when it built a small fingerprint scanner into its HP IPAQ H5450 PDA (Williams p1)

Hand Geometry

As you guessed, hand geometry is a biometric solution that reads a persons hand and/or fingers for access.

Hand geometry may be familiar to you if you have ever been to a Walt Disney World theme park. Prior to entering the theme park, a user aligns the palm of his or her hand and fingers onto a metal surface with guidance pegs that read the hand and finger attributes of that person. In conjunction with your paid admission ticket, the device then records the users hand information and sends it to its database for identification and verification for entering and reentering the park. Like fingerprinting, this is usually a 5 second process. (Individual Biometrics 2002)

Hand geometry offers many advantages similar to the other technologies such as ease of use, small data collection, resistant to attempt to fool a system, difficult technology to emulate a fake hand, and provides for the elimination of buddy punching in workforce management solutions.

There are however several challenges to the technology. Besides high proprietary hardware costs and size, the aging of the hands and fingers of individuals poses a challenge. The inability of the machines to cater to those with hand injuries is a second challenge; the lack of accuracy of the technology can be seen as a third challenge, and the final challenge deals with the biometrics inability to not recognize a fake hand. If the right pressure is applied to the surface correctly, this can be done with relative ease. As mentioned, this has proven to be extremely difficult. (Individual Biometrics 2002)

The future of hand scanning appears to be static. From a cost standpoint, is more expensive then fingerprint technology and just as effective. In the case of a workforce management solution, hand punch terminals are not as reliable since hand scanners are predominantly used for verification purposes only. If used in conjunction with other techniques, passwords, and smart card and tokens then it could prove to be a viable method.

A Hand Geometry Example:

Corporations such as Time Masters, Inc, out of Los Angeles, California, have specialized in this technology and have marketed hand and finger geometry as a part of a workforce management solution for companies. The Time Masters Hand Punch (Figures E and F) captures a three-dimensional accurate image of an

employee's hand each time an employee punches in and out with green and red lights notifying the employee of the status of each punch. (6)

Figure E: Time Masters Hand Punch

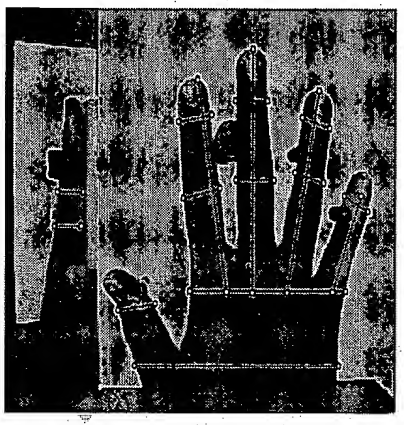


Figure F: HP Hand Position

Facial Recognition

As gathered from the name, facial recognition analyzes the characteristics of a person's face. Access is permitted only if a match is found. The process works when a user faces a digital video camera, usually standing about two feet from it, where the overall facial structure, including distances between eyes, nose, mouth, and jaw edges are measured. These measurements are retained in a database and used as a comparison when a user stands before the camera again. (Individual Biometrics 2002)

Facial recognition has many advantages such as easy integration into existing access control or time and attendance systems; verification and/or identification being accomplished in a short time period; flexible communication interfaces that enable terminals to be networked together; and a non-intrusive technology.

Facial recognition technology does have its challenges. Today's IT and Security professional will have to deal with the frustration of verification reattempts. Changes in lighting, objects in the background distorting a reading, imprecise facial positioning, and expressions of the user can all contribute to verification reattempts. A second challenge is the scanners inability to recognize countermeasures against a clean photo such as beards, mustaches, and disguises. A third challenge is the possibility of fake faces or molds affecting a reading. Legal and privacy issues can be seen as final challenges. (7)

The future of facial recognition remains uncertain due to the difficulties in making a positive identification of a person and with this biometric being a verification-only type of system. Since its inception, facial recognition has been touted as a fantastic system for recognizing potential threats (whether terrorist, scam artist,

or known criminal) but so far has been unproven in high-level usage. The technology has proven to have more problems than successes.

A Facial Recognition Example:

Cognitec Corporation's FaceVACS-Entry technology facial recognition scanner (Figure G) showcases a facial recognition example. Here the technology is used for allowing this flight attendant airport access and verification. Notice the distance (2 ft) from the machine to the user. (8)

Figure G: Cognitec FaceVacs

Iris Scanning

Iris scans analyze the features that exist in the colored tissue surrounding the pupil of an eye – the iris. It involves a user, as close as a couple of inches and up to 2 feet away, looking into a device where their iris is scanned and compared. The comparison is conducted at more than 200 points and checked for similar rings, furrows and freckles of the eye. (Individual Biometrics 2002)

The main advantage of iris scanning involves the extreme accuracy of the technology. Since no two irises are alike, identification and verification are done with confidence. Iris scanning also involves non-invasive technology; an ease of use since irises cannot be stolen, unlike keys, access cards, and password systems; and eliminates the frustration for users to have to remember passwords. In addition, and unlike the other techniques learned thus far, will recognize a fake eye from a real one by varying the light shone into the eye and watching for pupil dilation. (Individual Biometrics 2002)

The main challenge of iris scanning involves its high cost. Over time, this should come down in price. Additional challenges involve the potential difficulty in getting someone to hold their head in the right spot for a scan, bad readings due to poor

conditions such as lighting, surface positioning if behind a curved, wet, or reflecting surface; and the possibility of obscured irises due to eyelashes or drooping eyelids. (Biometric security systems p 20)

The future of iris scanning appears to be very bright as the ease of use and accuracy of the technology will open the doors for iris scanning in correctional facilities, county jails, airports, banks, and police stations around the country. It is very possible that in the near future everyday people will use iris scanners on a daily basis for entering the office and logging onto corporate networks. Parole officers can use the technology for verifying their paroles; government officials can use it to prevent welfare recipients from using different names and receiving twice the allotted welfare; and ordinary people can use it as a means of an electronic signature for online purchases and business documents. (9)

An Iris Scanning Example:

Corporations such as Iridian Technologies have taken advantage of iris scanning with the development of their very own proprietary architecture and camera software. The Iridian iris recognition technology reaches the marketplace in cooperation with iris-enabled camera (Figures 2,3,4) manufacturers and distribution with licensees such as Panasonic, Oki, and LG. (10)

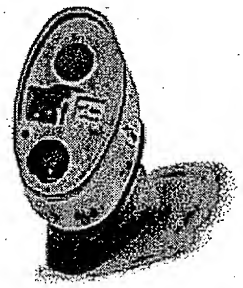


Figure 2.

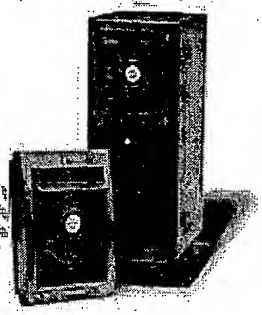


Figure 3.

Figure 4.

Iridian Technology Iris Scanners (Figure 2 – Windows based Workstation iris scanner, Figure 3 – Physical access reader, Figure 4 – ATM machine, where an iris is used in place of a PIN number) (Chang p3)

Retinal Scanning

Retinal scanning devices are the most accurate physical biometric available today since there is no known way to replicate a retina. Similar to iris scanning, retinal scanning analyzes the layer of blood vessels at the back of the eye. The scanning involves using a low-intensity light source and an optical coupler that reads the patterns of a person's retina.

Still relatively new and primarily used for high-risk security areas, its popularity is gaining acceptance. Retinal scanning has a user look through a small opening in the device at a small green light. The user must keep their head still and eye focused on the light for several seconds during which time the device will verify his or her identity. This process takes about 10 to 15 seconds total. (Individual Biometrics 2002)

Besides being the most accurate biometric technique available, retinal scanning provides for several additional advantages. The first advantage is the capability of providing viewing assistance to those who are visually impaired (Figure H); a second advantage is providing a piece of mind in knowing the technology is 100% accurate, and the final advantage of the technology being seen as a great long term cost alternative to some other biometric techniques. (Biometric Security Systems web p23)

Besides cost, several challenges to this technology exist. They include the invasive screening process and user discomfort. For example, it requires a user to stand within inches of a device to get an accurate reading, it requires a user to remove glasses if they wear them, it requires a user to place their eye close to the retinal scanning device, and it requires a user to focus on a certain point for a certain period of time.

The future of retinal scanning appears bright. However, it needs to be more refined, non-intrusive, and cost effective for acceptance. I think over time you will see a decrease in the costs and more marketing of the products and technology.

Retinal Scanning Examples:

Corporations like Microvision (11) have capitalized on retinal technology and specifically in offering it as an alternative to helping those who are visually impaired (Figure H). Through a small device called Nomad (Figure I), people will be able to read information from a small, wearable computer that projects an image over their normal vision. The display is a red, transparent computer screen, but, in fact, is no screen at all. The device shoots a tiny laser beam that draws patterns onto the retina so that only the wearer sees the images. (12)

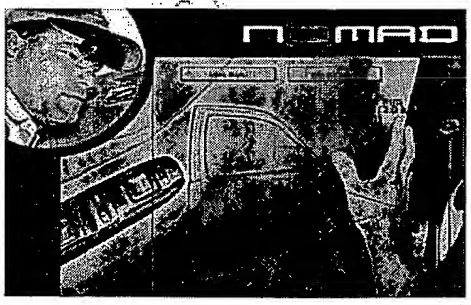


Figure H: Microvision

Figure I: Nomad User

Figure J: Retinal Tech

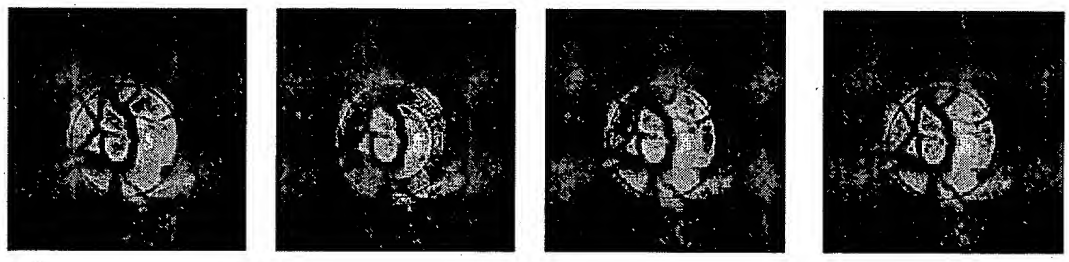


Figure K: Retinal Tech scanning process

To illustrate the retinal scanning process, Retinal Tech Corporation offers a retinal scanning device (Figure J) that scans a person's retina in four distinct and different phases (Figure K). This technology is designed to be extremely versatile for attachment to a door for physical access, incorporation into a wand, kiosk, or ATM machine, and for connection to a computer. It also works outdoors, in low lighting, and is hands free. (13)

Vascular Patterns

Vascular patterns are best described as a picture of the veins in a person's hand or face. The thickness and location of these veins are believed to be unique enough to an individual to be used to verify a person's identity. (Individual biometrics 2002)

The most common form of vascular pattern readers are hand-based such as Techsphere Corporation (Figures L and M), in requiring the user to place their hand on or in a curved reader that takes an infrared scan of their veins. This scan creates a picture that can then be compared to a database to verify a user's identity. (14)

Figure L: Techsphere Company Scanner

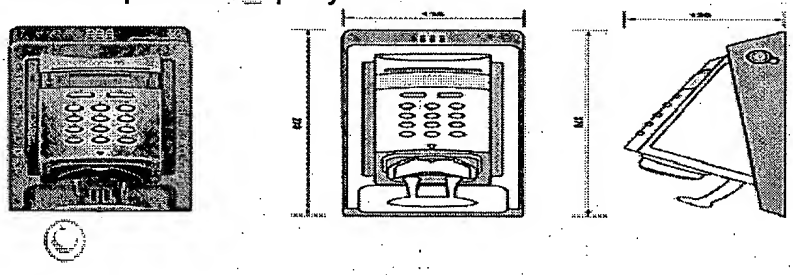


Figure M – Techsphere Company Reader

Too new to have much data, vascular pattern technology does seem to have a few advantages over its counterparts, including the great difficulty in emulating another person's vein structure, and not having to worry about rain, glasses, or external injuries. (Individual Biometrics 2002)

Challenges do exist in the medical community. Medical testing such as the effects of aging, heart attacks, and medical problems with one's arteries on the scans has yet to be determined fully. It also requires a large amount of space to mount the device so that the entire hand can be scanned; which may restrict its usability. (15)

The future of vascular pattern recognition appears to be very bright. Though minimally used at the moment, vascular pattern scanners can be found at major military installations, some multi-outlet retailers, and currently as a means of gun control. The scanner is built into the guns handle so when an authorized person grabs the handle the firing mechanism is automatically unlocked enabling them to shoot. (Biometric Security Systems p24)

A Vascular Pattern Example:

UK researchers have developed the SIA scope (Figure N) for vascular recognition technology to help aid in the early detection of skin cancer - the first noninvasive system to be able to "look" beneath the surface of the skin. By using it, doctors can rapidly tell the difference between skin cancer and other types of skin damage. This allows the cancer to be identified earlier and treated more quickly, and with greater success.

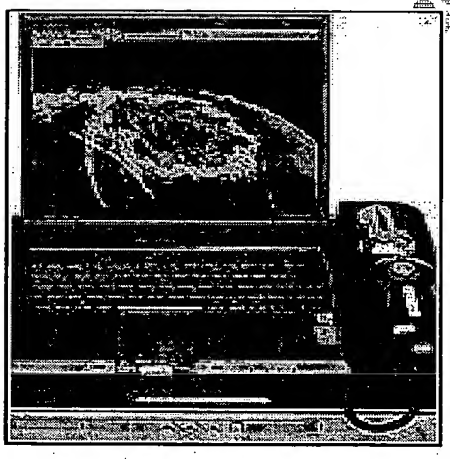


Figure N: the SIA scope

Based on a scanning technique using harmless light, in a sequence of visible (red, green and blue) and infrared wavelengths from 400 to 1,000 nanometers, light interacts with tissue in different ways depending on the composition of the tissue.

The SIA scope measures the amounts of the different frequencies of light that are absorbed, scattered and reflected by skin.

Computer software uses a mathematical model to compare the reflectance properties with the results expected from normal skin tissue. Subsequently, it constructs images that show the tissue composition at more than 350,000 points in the skin within a scan area of 11-millimeter diameter to a depth of about 1,000 nanometers (one micro-meter), enabling a doctor to detect early signs of cancer or recognize other skin complaints.

The system completes a scan in under five seconds and processes the data to create a series of images in about 10 seconds. These SIA graphs as they are known (which can also include 3D representations) image the concentrations of melanin, dermal melanin, blood and collagen in the scanned area. (16)

Here are some behavioral biometric techniques.

Behavioral Biometric Techniques

Speaker Recognition Software

Speaker recognition software has been around for quite a while and is beneficial for those utilizing speech and voice as a means of authentication. Speaker recognition involves a user speaking into a microphone with his or her password or access phrase. Here, systems are able to filter out background noise and take into account microphone variances. Verification is confirmed via a database from a previously recorded voice and takes approximately 5 seconds to complete. (Individual Biometrics 2002)

There are several speaker recognition verification systems to consider. They include Fixed Phrase Verification (subject uses the same phrase to access a system), Fixed Vocabulary Verification (designed to prevent the recording of passwords, incorporates a limited vocabulary often using PIN numbers for access), and Flexible Vocabulary Verification (fixed or prompted strings of words can be used as pass phrases). (Biometric Security Systems p24)

To prevent recorded voice use, most devices require the high and low frequencies of the sound to match, which is difficult for many recording instruments to recreate well.

Advantages of speech recognition technology include the flexibility to record and accept multiple verifications, speech, and multiple languages; the inexpensive cost and implementation (easily deployable since a telephone and microphone are used); ease of use, and its acceptance. The challenges of this technology deal with it being unaccommodating to the hearing impaired, as well as, the potential of using recorded voices as a breach of access. (Woodward p4)

The future of speaker recognition continues to be bright. You will see more and more applications for controlling access to computer networks (add this to usual password, token, or smart card authentication) or websites; automated password reset services; transaction authentication for telephone banking, and electronic and mobile commerce; for home parole monitoring and prison call monitoring; in voicemail browsing for labeling incoming voicemail with speaker name; and for personalization of voice-web or device customization. (17)

A Speaker Recognition Example:

The Scan Soft TTS-2500 is part of the Scan Soft Corporation Speech Solutions product range and is a high-quality solution to enable speech to virtually any device through the integration of a broad range of features onto a single chip.

The product allows developers to speech enable devices for talking clocks, household appliances, navigation aids, talking books, answering machines and voicemail systems, talking dictionaries, language translators, security system monitors, and cell phones to industrial warning system controls and educational electronic learning aids.

All devices allow for very competitive prices with applications providing multilingual (available in 5 languages: American English, French, German, Spanish, and Mandarin Chinese) options and unlimited system vocabulary in selectable male, female, and customized voices. As well as, providing high accuracy, advanced speech algorithms, low cost, and superior quality. (18)

Signature Recognition

Is an automated method of measuring an individual's signature by having a user sign on a tablet or on paper that is lying over a sensor tablet. The device records the signature and compares it to its database. (Individual Biometrics 2002)

The technology examines such dynamics as speed, directions, and pressure of writing; the time that the pen or stylus is in and out of contact with the paper, the total time taken to make the signature; and where the stylus is raised and lowered on the paper. (Woodward p4)

The advantages of signature recognition include being able to accommodate to those who have trouble speaking, ease of use, easily deployable, and low development and application costs.

It does have several challenges. The obvious choice involves the inability of the technology to cater to those with difficulty writing and the inability of adjusting the technology to cater to those using foreign languages. Because of this, the future of signature recognition remains static. If you are a global corporation, you may want to opt for other biometric alternatives.

A Signature Recognition Example:

Companies such as Automated Signature Technology have revolutionized signature recognition with several customized products.

They have developed signature recognition automatic pen and ink signature machines that alleviate the task of signing letters. In addition, they allow you to sign your name with any kind of pen desired.

Here, Figures O and P showcase two Automated Signature Technology signature recognition types. (19)

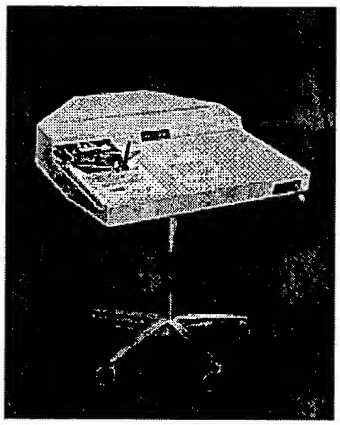


Figure O: AST SR #1

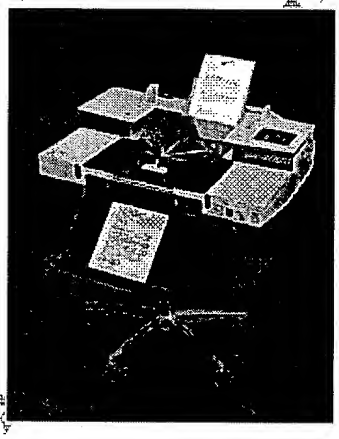


Figure P: AST SR #2

Keystroke Recognition - 9

Involves a user typing his or her password or phrase on a keyboard. The system then records the timing of the typing and compares the password itself and the timing to its database. Verification takes less than 5 seconds. (Individual Biometrics 2002)

This technology examines such dynamics as speed and pressure, total time taken to type certain words, and the time elapsed between hitting keys. It also involves measuring successive keystrokes, keystroke durations, finger placement and applied pressure on the keys from that user. (Woodward p5)

The advantages of keystroke dynamics in the computer environment are obvious. Neither enrollment nor verification disturbs the regular workflow because the user would be tapping the keys anyway. And unlike other biometrics systems, keystroke dynamics is almost free. The only hardware required is the keyboard and using the software is no more difficult than typing ordinary passwords. (20)

Analysts who follow the biometrics industry say the keystroke technology is less accurate than other technologies such as fingerprinting or retinal scans and has gained little acceptance. Thus, the future of keystroke recognition remains uncertain.

A Keystroke Recognition Example:

This keystroke recognition technology has recently gained notoriety in the music industry. Start-up Musicrypt.com and Net Nanny Software said they are joining forces to create software that can identify individual music listeners by the way they tap out letters on computer keyboards. This information would be used to protect songs against unauthorized distribution and use.

The companies want music labels or online retailers to insert the technology into downloaded music, so that only a person who buys a given song would be able to play it on a computer. Identifying the buyer by these keystroke patterns is far more secure than using passwords, which can be passed on to thousands of people. (21)

Biometrics of the Future

Are infinite in their possibilities. Many of the technologies discussed thus far are paving the way of the future. However, newer technologies (gait recognition, lip print identification, body odor) are gaining more and more acceptance.

In the medical world, gait recognition, which measures body gestures and movements, is being used by physical therapists to help detect and remedy human movement patterns. It may someday revolutionize the way we are allowed access to places. This behavioral biometric technique recognizes the uniqueness in the ways people walk by scanning human movement, then digitalizing (via binary transfer) the data, and storing the data for a match. It can detect, classify, and identify humans from distances up to 500 feet away and under all weather conditions in both day and evening. Its accuracy remains a current drawback. (Shen p11)

In the forensic science community, the use of Lip Print identification is gaining more acceptances. Similar in the logic of fingerprinting, lip prints provide an alternative form of identification. The hassle of reading ones lips and piercing issues prove to be challenges. The main drawback is the user effort required for authentication. (Shen p14)

Body odor recognition (also called chemical odor analysis) is seen as another biometric. Yet still unproven, we know that certain breeds of dogs excel at using their sense of smell to track humans. At least one company is working on a device to identify people based on body odors. The scientific basis of the work is that the chemical composition of odors can be identified using special sensors.

The University of Leeds has pioneered similar research that has application to drug and bomb detection technologies. The disadvantages of this technology include inconsistencies in chemical composition resulting from hormonal or emotional changes. (22)

The main obstacles of biometrics will continue to involve complexity and privacy issues surrounding information abuse. Biometric information abuse has caused some civil libertarians to be incensed by the risks posed by the personal nature of biometric information and how this information can be manipulated or misused for unimaginably evil purposes by other people, employers, and governments. Additional concerns center around biometric accuracy and performance – vendors need to be able to commit to a 100% accuracy of their technologies, something that they do not want to do at this time; many of the biometric techniques are easy to fool such as the case of a fingerprint saved on a piece of candy; and systematic bypass of determined and creative hackers. In other words, today's hacker is becoming smarter than ever. (23)

Physiological biometric technology and finger scan technology (36%) will continue to dominate the biometric market. However, other technologies such as hand 27%, signature 5%, iris 16%, voice 6%, and facial 11% recognition are all gaining popularity. And handwriting technology is becoming popular with banks and credit card authorizations. (Shen p6)

The future of biometrics depends upon its industry. The biometric industry must first shed the negative media perceptions of the technologies. It must change the perceptions of an immature and standards developing market. It must improve the engineering of biometric applications and show a better return on investment to corporations. And most importantly, it must improve its growth by eliminating the privacy perceptions and legal issues that exist. (24)

Biometrics usage will continue to work in conjunction with security software (firewalls, antivirus, encryption) and security hardware (token and smart cards, and firewall/VPN devices); in security sensitive environments such as airports and casinos; with law enforcement; prisons, jails, amusement and theme parks, corporate time systems, in assisting the disabled and mentally challenged; with new technologies for laptops not communicating with a corporate network; on desktops communicating with a corporate network; and more vendor product and service line expansion. The popularity of e-business will continue to be the driving force behind advanced security needs. (Shen p6)

When choosing a biometric system, the following items should be considered when deciding. Characteristics such as speed, accuracy, user-friendliness, low-cost, public acceptability, reliability, resistance to counterfeiting, acceptable storage requirements, and fast enrollment times should all be considered. (Network Security 2003)

Overall, I hope this paper has exposed you to a vast future of opportunity that exists in physical security and biometrics. The intent was to showcase and discuss the myriad biometric techniques available today and tomorrow, highlight the advantages and disadvantages of these techniques, illustrate key company and contact information if interested in implementing them, and to provide you with assistance and considerations with choosing the right biometric solution.

Bibliography

1. Woodward, John. "Biometrics: A look at Facial Recognition"; October 2003. http://www.rand.org/publications/DB/DB396/DB396.pdf

2. Individual Biometrics. "An Overview of Biometrics", June 2002 http://ctl.ncsc.dni.us/biomet%20web/BMIndex.html,

3. Precise Biometrics. "Personal Proof: Knowing who's who when security really counts", November 2003. http://www.precisebiometrics.com/data/content/DOCUMENTS/200359141913709Personal_Proof_2003.pdf

4. Biometric Security Systems. "Biometric Technologies", November 2003. http://www.biometricsecurity.com.au/technologies/technologies.htm

5. Williams, Martyn. "Casio Unveils Better Cell Phone Security", http://pcworld.shopping.yahoo.com/yahoo/article/0,aid,109597,00.asp, Yahoo; Feb 28, 2003.

6. Time Masters Corporation website. Product Family. October 2003. http://www.time-masters.com/jjj.php?family=100

7. Penman, Richard. "The Role of Facial Recognition: Biometrics in the Security Industry", Geocities, July 6, 2002. http://www.geocities.com/penmanre/Research/FacialRecognitionBiometrics.htm

8. Cognitec Systems. Product Family. November 2003. http://www.cognitec-systems.de/products-entry.htm

9. Chang, Ellen. "Iris Scanning", Research Paper, Dec 8, 2000. http://www.stanford.edu/~ellenc/cs147/IrisScanning.htm

10. Iridian Technologies. Product Family. November 2003. http://www.iridiantech.com/products.php?page=4

11. Microvision Corporation. Home Page. November 2003 http://www.microvision.com

12. Heckman, Candace. "Eyesight of the future is here". June 18, 2001. http://seattlepi.nwsource.com/business/27731_retina18.shtml

13. Retinal Technologies. Technology. November 2003. http://www.retinaltech.com/technology.html

14. Techsphere Corporation. Products. November 2003. http://www.tech-sphere.com/english/system.htm

15. Shen, Michelle M. "The Promise of Future Technologies", June 26, 2003. BiometriTech: 2003 NY Conference and Exposition. http://www.epolymath.com/futuretechnologies.pdf

16. Welsh, David. "Non-Invasive technology looks beneath the skin", October 25,2003. Dawn weblink, http://www.dawn.com/2003/10/25/index.htm

17. Reynolds, Douglas "An Overview of Automatic Speaker Recognition Technology", Applications. July 10, 2002 http://www.clsp.jhu.edu/ws2002/preworkshop/reynolds.pdf,

18. Scansoft Corporation. Real Speak TTS-2500 Product Information. November 2003. http://www.scansoft.com/realspeak/tts2500/

19. Automated Signature Technology. Products. November 2003. http://www.signaturemachine.com/products/products.html

20. Schaup, Sonja "Computer user verification based on keystroke dynamics", Cryptology and Data Security. November 2003. http://cs.fernuni-hagen.de/researchAreas/cryptology/main_Computer_User.html

21. Borland, John. "The latest in anti-piracy efforts: Keystroke Recognition", news.com, June 13, 2000 http://news.com.com/2100-1023-241792.html?legacy=cnet

22. Network Security Technologies. Presentation. November 2003 http://www.cs.usask.ca/undergrads/der850/project/biometrics/methodologies.shtml

23. Yudkowsky, Chaim. "Body of evidence suggests increased use of biometrics", Triangle Business Journal, October 2003 http://triangle.bizjournals.com/triangle/stories/2003/10/06/smallb3.html,

24. Huddart, Martin. IBIA: Biometrics Advocacy Report. October 3, 2003. http://www.ibia.org/newslett031003.htm

news

January 21, 2004

FOR IMMEDIATE RELEASE
Editorial Contact: Richard Hahn
(716) 372-2443 (rich@richardhahn.com)

Eran Basis Joins Barantec as Managing Partner

Eran Basis

Ayal Vogel

Eran Basis has joined Barantec as a managing partner. With his experience and knowledge in engineering, Basis will head the engineering department as a liaison for product development between the Research & Development in Israel and customers in the United States.

In addition, Basis will be responsible for the internal operations of the company, which will allow managing partner, Ayal Vogel to concentrate on business development.

"I'm excited to be on the Barantec team and the opportunities that lie ahead of us," said Basis. "I'm also looking forward to working closely with the manufacturers in the industry and introducing new products to the market."

With his background, Basis is perfectly suited to head the engineering department. Since many of the projects in the EverSwitch arena, as well as the access control world, require tight engineering collaboration, Basis will facilitate this interaction locally along with the resources of the Research & Development department overseas. Barantec is hopping that this addition will dramatically shorten the "time to market" factor for new product development as well as improve the technical support for existing products.

Before joining Barantec, Basis worked in the R&D department for several different companies. In 1989, he founded Solutioneering Inc, an engineering consulting company with two other partners. .

"Eran has been a close personal friend and I know that he will be a great asset to the company as we move forward into the future and in our ongoing effort to increase our support, develop new products and most importantly, to better serve our customers," said Vogel.

Basis may be reached at 973-779-8774 or by e-mail at eran@barantec.com. For more information, contact Barantec, Inc., Plaza 777, Passaic Avenue, Clifton, NJ 07012. Phone (973) 779-8774; Fax (973) 779-8768; Info@barantec.com, web site www.barantec.com.

Barantec is a NJ based corporation and a subsidiary of The Baran Group, a publicly traded conglomerate comprised of 13 different companies with over 1,000 employees worldwide. With the resources of a $150,000,000 global concern, Barantec acts as the investment and business management vehicle for a variety of The Group's activities in North America. Barantec markets a variety of unique, patented products and continue to develop "cutting edge" solutions with extensive and on-going R&D efforts.
###

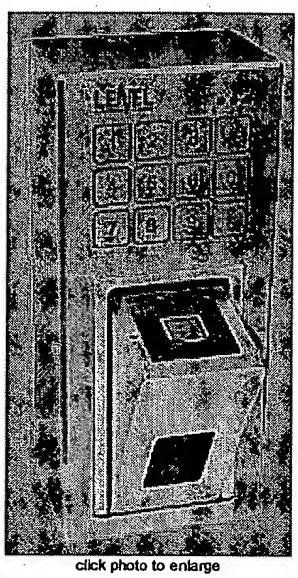
January 5, 2004

FOR IMMEDIATE RELEASE
Editorial Contact: Richard Hahn
(716) 372-2443 (rich@richardhahn.com)

Barantec and Lenel Produce Virtually Indestructible Biometric Access Control Unit

Barantec, Inc. and Lenel Systems International, Inc. have combined forces to produce BIOGuard, the most rugged biometric access control unit with three-factor authorization and a three-tier security line of defense.

The new BIOGuard combines a keypad, proximity reader and biometric unit and can be set up for one, two or three factor authorization. While most security system architecture uses biometric authentication alone or along with a proximity, there are none that take advantage of a three-factor authentication and none where the biometric fingerprint sensor is protected until authorization from both the PIN number and proximity reader.



click photo to enlarge

The common biometric readers is vulnerable to vandalism, which is why Lenel decided to hide the most expensive part of the reader so that only a valid user, who wouldn't damage the sensor, could have access. It is set up so that a mechanical door encases the biometric reader and only opens on authorization. The power-driven fingerprint sensor, utilizes a powerful DSP TI processor, Bioscrypt's MV1200.

Lenel chose to use Barantec's Everswitch technology and their virtually indestructible keypads as the "shell" for the unit because they are easy to install, vandal proof, aesthetically pleasing and impervious to the elements. Fully immersible and able to work under water, the keypad is able to withstand user abuse, the harshest environments and temperatures ranging from –31 degrees to 150 degrees F. With a standard Wiegand output, Barantec's Everswitch keypads are compatible with most access control systems.

"There is a vulnerability with mechanical and membrane keypads," explained Vogel. "As we worked closely with Lenel who wanted to add biometrics, to their product line, we both realized that the biometric fingerprint sensor would be susceptible to damage. It was not so much that the sensor would fail and someone could get inside but that someone could damage the fingerprint lens and cause failure."

Lenel has been working closely with Barantec and already has a number of strategic agreements in place. The company sells standard Barantec keypads products as an addition to their access reader line and is also reselling some OEM products including the Everswitch Prox and the Everswitch iClass for HID, as well as BIOGuard reader.

"We designed the BIOGuard with Barantec in mind because they had the ability to integrate the necessary technologies into the most rugged package yet keep it aesthetically pleasing," said Robert Pethick, manager of hardware platforms for Lenel. "Barantec has recently come from an industrial industry to the security industry where we could have used them three or four years ago. They have generated a name for themselves, especially with the FAA contract for cockpit doors that they secured, and have opened up the eyes of the security industry to our vulnerabilities, introducing us to a new set of enclosure solutions."

June 9, 2003

FOR IMMEDIATE RELEASE

Editorial Contact: Richard Hahn
(716) 372-2443 (rich@richardhahn.com)

Barantec Combines Its Virtually Indestructible Keypad with HID's iClass Smart Card Reader

With the success of the Everswitch Prox, Barantec and HID are taking another step forward and launching the Everswitch iClass, a combination of Barantec's virtually indestructible metal keypad with HID's 13.56 MHz contactless smart card reader.

For the first time, the security industry can offer end users additional security measures for dual verification with a unit that's built specifically for high traffic areas and harsh environments. Both components are vandal proof and the card reader unit is uniquely built into the keypad as one integrated piece, not simply attached to its perimeter.

"With the Everswitch iClass," said Barantec president, Ayal Vogel, "we are again offering the best of both worlds and changing the way the security industry thinks about readers. The current standard plastic mechanical readers are less secure than Barantec's all metal, non-mechanical solution to access control. Plus, the lifetime warranty, anodization and multi colors sets Barantec apart from all other access manufacturers.

The Everswitch iClass is easy to install, vandal proof and impervious to the elements. It is fully immersible and can work under water. The unit is able to withstand user abuse, the harshest environments and temperatures ranging from -4 degrees to 158 degrees F. With a standard Wiegand output, the Everswitch iClass is compatible with almost all access control systems.

Barantec's "Everswitch Inside" logo represents the company's patented piezo technology. The piezoelectric effect is the property exhibited by certain crystals of generating voltage when subjected to pressure and conversely, undergoing mechanical stress when subjected to an electric field. The sensors embedded below the metal surface of the keys are made of a ceramic alloy that only needs pressure to activate. There are no moving parts to wear out and all numbers are hard anodized for years of use without wear.

The Everswitch iClass is perfect for high security traffic areas such as airports and government buildings. And while mechanical keypads often have grime and dirt that infiltrate the unit, the Everswitch iClass is flat, easy to maintain and ideal for hospitals where hygiene is a concern.

"The Everswitch iCLass is also a perfect solution for architects, engineers and consultants because this gives them the opportunity to think outside the box. They can customize this product in ways that they've never been able to before," added Vogel. "Typically, the security industry provides only a black or gray option, but the Everswitch iClass can be colored to match the pantone selection of any décor and the keypad's anodized graphics never wear off."

The Everswitch iClass is the second product that Barantec and HID have introduced. The strategic partnership has already produced the Everswitch Prox, which combined Barantec's piezo keypad with HID's prox unit. The Everswitch Prox won the Security Industry Association's New Product Showcase award in the access control category at ISC West 2003.

Both companies have high expectations that the Everswitch iClass will be received by the industry with the same enthusiasm.

For the future, Barantec is continuing to look for new ways to apply their patented Everswitch technology including a biometric solution that will be released soon.

For more information, contact Barantec, Inc., Plaza 777, Passaic Avenue, Clifton, NJ 07012. Phone (973) 779-8774; Fax (973) 779-8768; Info@barantec.com, web site www.barantec.com.

Barantec is a NJ based corporation and a subsidiary of The Baran Group, a publicly traded conglomerate comprised of 13 different companies with over 1,000 employees worldwide. With the resources of a $150,000,000 global concern, Barantec acts as the investment and business management vehicle for a variety of The Group's activities in North America. Barantec markets a variety of unique, patented products and continue to develop "cutting edge" solutions with extensive and on-going R&D efforts.
###

November 15, 2002

FOR IMMEDIATE RELEASE
Editorial Contact: Richard Hahn
(716) 372-2443 (rich@richardhahn.com)

Baran/Tec Combines Virtually Indestructible Keypad with HID Proximity Reader

Baran/Tec, Inc. has recently introduced the Everswitch Prox, a combination of a virtually indestructible metal keypad with an HID proximity reader, giving end users the best of both worlds for the first time.

With the Everswitch Prox, the security industry now has the option of an easy to install, vandal proof, waterproof and weatherproof keypad and prox reader that has no external housing and requires no maintenance or repair for their access control systems.

By utilizing a patented solid-state piezo design in the Everswitch Prox, Barantec has developed a totally sealed, all metal product that has no moving parts and therefore boasts unprecedented life expectancy and can be combined with proximity control for added security. The totally sealed, all-metal construction meets and exceed most standards and is ideal for high traffic, hazardous or extreme user pattern applications.

In the past, the security industry has used stand-alone plastic proximity units and avoided mechanical keypads in high traffic areas, which are susceptible to vandalism, excessive use and the elements.

The sensors embedded below the metal surface of the Everswitch Prox are made of a ceramic alloy that only needs pressure to activate. There are no moving parts to wear out or tampered with. All numbers are hard anodized for years of use, lasting to an excess of 50 million cycles. No one will ever be able to figure out a pin number based on the wear on the keypad.

The Everswitch Prox is able to withstand user abuse, the harshest environments, as well as intrinsically safe environments, and temperatures ranging from -4°F to 158 °F. And since the Everswitch Prox is totally sealed, the unit is waterproof, dustproof and there is no concern with radio interference.

"One of our Everswitch keypads was shot with a 9mm gun and it still worked," said Barantec president, Ayal Vogel. "Even if it takes an indirect hit from a bomb blast, the chances are it has a good chance of continuing to operate."

The piezoelectric effect, discovered by the Curie brothers in 1880, is the property exhibited by certain crystals of generating voltage when subjected to pressure and conversely, undergoing mechanical stress when subjected to an electric field. That technology makes piezo products perfect for high security traffic areas or where there is concern over vandalism.

While the Everswitch Prox may be in excess for what is needed for residential applications, it does have a place in the high-end market because of its clean look and aesthetics. While mechanical keypads often have grime and dirt that infiltrate the unit, the Everswitch Prox is flat and easy to maintain and not affected by chemicals.

"Most of the security industry is not familiar with keypads that are virtually indestructible.
The Everswitch line, which is currently being used in airports, schools, hospitals, vending machines, medical equipment, information kiosks, mining equipment and a variety of other applications, will open up new opportunities in a variety of applications. Security professionals should look for piezo technology and the "Everswitch Inside" logo in their next keypad," added Vogel.

For more information, contact Baran/Tec, Inc., Plaza 777, Passaic Avenue, Clifton, NJ 07012. Phone (973) 779-8774; Fax (973) 779-8768; Info@barantec.com, web site www.barantec.com.
Baran/Tec is a NJ based corporation and a subsidiary of The Baran Group, a publicly traded conglomerate comprised of 13 different companies with over 1,000 employees worldwide. With the resources of a $150,000,000 global concern, Barantec acts as the investment and business management vehicle for a variety of The Group's activities in North America. Barantec markets a variety of unique, patented products and continue to develop "cutting edge" solutions with extensive and on-going R&D efforts.
###
October 14, 2002

FOR IMMEDIATE RELEASE
Editorial Contact: Richard Hahn
(716) 372-2443 (rich@richardhahn.com)

FAA Approves Baran/Tec Keypad for Securing Cockpits

New Electronic Entry System Includes only FAA Certified Access Control Keypad in the Security Industry

Baran/Tec, Inc. was recently awarded FAA Certification for the company's new Cockpit Door Access Control Keypad, giving them the only certified keypad for flight deck doors in the security industry.

A key benefit of the new keypad is its ruggedness and reliability. Its totally sealed, all-metal construction makes it ideal for hazardous or extreme user pattern applications. By utilizing a patented solid-state piezo design, Barantec is able to manufacture totally sealed, all metal products that have no moving parts and therefore unprecedented life expectancy.

The piezoelectric effect, discovered by the Curie brothers in 1880, is the property exhibited by certain crystals of generating voltage when subjected to pressure and conversely, undergoing mechanical stress when subjected to an electric field. Piezo products are perfect for high security traffic areas or where there is concern over vandalism.

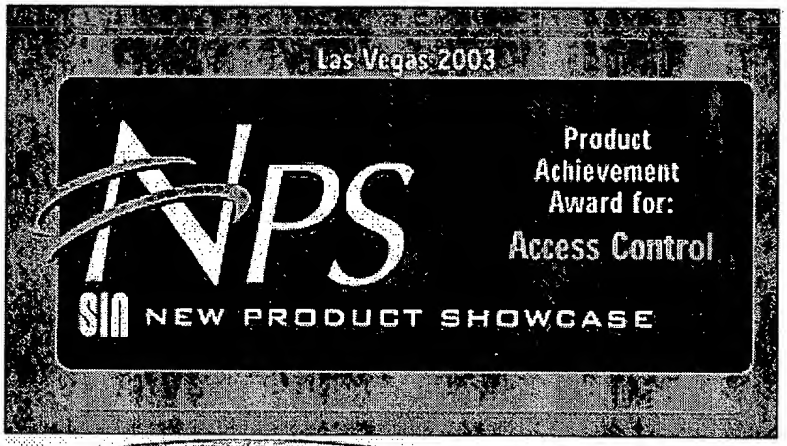
Barantec worked closely with Timco Aviation Sales of Greensboro, NC, a maintenance repair organization with FAA approved personnel on their staff, to develop the unique software and receive FAA approval.

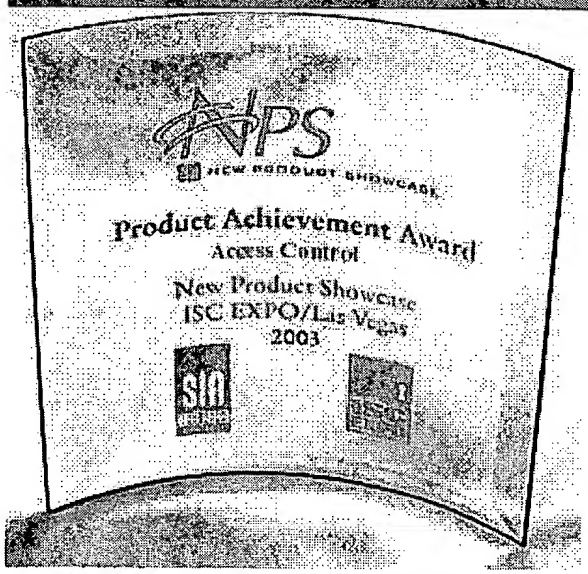
The keypad is part of a complete flight deck door solution that also includes a reinforced panel door and a locking device. The new system is scheduled to be installed in the fleet of at least two major airlines and three secondary airlines within the next six months.

Ayal Vogel, Barantec's president said, "The rigorous FAA certification of our new access control keypad is another milestone in our continuous new product development and a great opportunity for Barantec to contribute to homeland security."

The Cockpit Door Access Control Keypad joins Barantec's complete line of security products that includes Wiegand keypads, Prox readers and single door access systems and crosses over into a host of other industries.

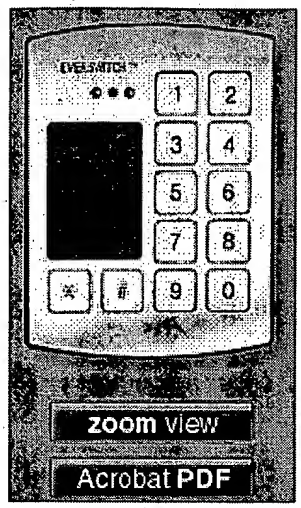
For more information, contact Baran/Tec, Inc., Plaza 777, Passaic Avenue, Clifton, NJ 07012. Phone (973) 779-8774; Fax (973) 779-8768; Info@barantec.com, web site www.barantec.com.
Baran/Tec is a NJ based corporation and a subsidiary of The Baran Group, a publicly traded conglomerate comprised of 13 different companies with over 1,000 employees worldwide. With the resources of a $150,000,000 global concern, Barantec acts as the investment and business management vehicle for a variety of The Group's activities in North America. Barantec markets a variety of unique, patented products and continue to develop "cutting edge" solutions with extensive and on-going R&D efforts.
###





learn what people are talking about....

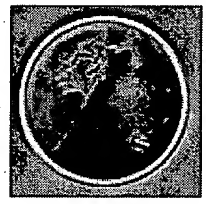
a combination of a virtually indestructible keypad with an HID proximity reader offering the security industry the best of both worlds **for the first time.**

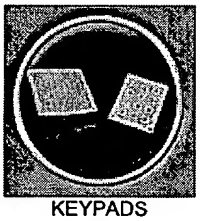


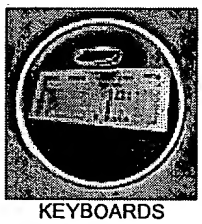
- Vandal Proof Tamper Proof
- Weather Proof (-4°F to 158°F)
- Water Proof and Dust Proof (IP68)
- Ideal for high traffic areas
- No moving parts (solid state construction)
- Anodized graphics that will never wear off
- Lifetime Warranty

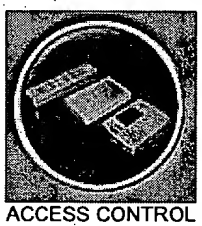
The keypad data output is available in various formats including 8, 26, and 32. The totally sealed, all-metal construction exceeds most standards and is ideal for high traffic areas.

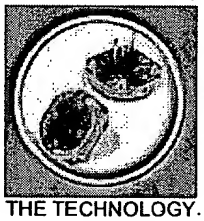
Compatible with most access control systems


SWITCHES


KEYPADS


KEYBOARDS


ACCESS CONTROL


THE TECHNOLOGY.

HOME | PRODUCTS | THE TECHNOLOGY | APPLICATIONS | NEWS | COMPANY INFO | CONTACT US

PRODUCED BY TECHNEWS 10 THE INDUSTRY JOURNAL FOR SECURITY PROFESSIONALS
JUNE 2004

Gemplus implements Verdicom's fingerprint matching algorithm on a smartcard

MAY 2000

Gemplus, the world leader in smartcard-based solutions and technologies recently announced that it had implemented Match-On-Card Technology, the new powerful fingerprint matching algorithm from Veridicom, on a low-end, 8 bit processor of a standard smartcard from Gemplus. This achievement allows to drastically enhance the security and the performance offered by a solution combining smartcards and fingerprint biometry since user's fingerprint template data never leaves the smartcard.

Fingerprint matching operations are entirely conducted on the smartcard itself in less than a second, unlike previous fingerprint authentication methods that required transfer of template information to a personal computer or workstation for matching leaving a potential security gap. Should the smartcard be stolen or lost, only a fingerprint match between the authorised user and the stored template unlocks the card preventing a lost card from being exploited by unauthorised users.

'Combo card' highly secure

This combination of 'what I have' (smartcard) and 'who I am' (fingerprint) is today recognised as one of the best solutions to secure Internet access and conduct electronic commerce transactions.

"This important partnership between Gemplus and Veridicom will produce the smart card of the future that eliminates the vulnerabilities associated with PIN numbers and any transfer of fingerprint templates," said Michael D'Amour, Veridicom President and CEO. "By bringing Veridicom's breakthrough fingerprint authentication technology together with the latest smartcard advances, this alliance will offer customers all the benefits of convenient smartcards that cannot be hacked."

"Gemplus is very enthusiastic to endorse Veridicom's technology at different levels, says Alexandre Lorenzi, Gemplus Corporate Hardware Director; the Veridicom sensor is indeed already implemented in both Gemplus contactless and contact readers ranges, respectively in partnership with BII and Precise Biometrics AB. Today, Gemplus is interested to embed a unique implementation of the Veridicom biometrics firmware within smart cards, to reach an ultimate security level in the whole biometrics process."

For details contact Severine Percetti of Gemplus on tel: (0933) 4236 6767 or e-mail: severine.percetti@gemplus.com

---

The Match On Card Technology

Magnus Pettersson

Precise Biometrics AB, Dag Hammarskjölds väg 2, SE 224 67 Lund, Sweden

22nd August 2001

Abstract

To make biometric verification secure, it is important to store the biometric data in a secure way. To be able to keep the biometric information in a closed environment, it is essential that the matching is performed in the same environment where the data is stored.

This document describes the Match on Card technology, and why the technology is needed to gain secure biometric verification. The document also discusses Match on Card in combination with smart cards and PKI.

1 Introduction

1.1 Biometric authentication

Biometric verification has the advantage of ensuring that only the correct physical user can gain access to certain information or areas. The biometric identity can never be borrowed, and it is up to the administrator of a system to decide who is to be granted access or not.

1.2 Enrolment and verification

During the enrolment (Figure 1), biometric data is captured. The data is processed, and a pattern is extracted. The pattern is chosen so as much unique information as possible is recorded. The extracted pattern is then stored as a biometric template.

During verification (Figure 2), a new pattern is extracted from the incoming fingerprint image. The pattern forms the fingerprint data that is matched against the stored template, containing the fingerprint information from the enrolment.

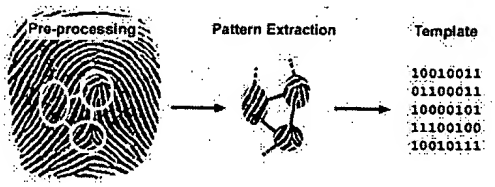


Figure 1: Enrolment.

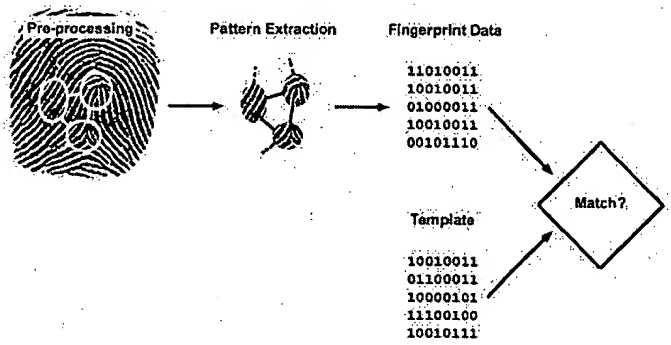


Figure 2: Verification.

1.3 Why do we need Match on Card?

To gain maximum security, the biometric template must be stored securely in a closed environment. If the biometric matching procedure is performed outside this closed environment it is exposed to the open environment, where anyone could steal the template. Even if the fingerprint template is protected by another security mechanism this is to be viewed as the weakest link, and the biometrics does not really add any security.

The only way to ensure that security is kept is to never let the biometric template leave the closed environment. In this case the biometric matching has to take place in this closed environment as well.

The Match On Card, MOC, technology solves this problem by performing the critical biometric matching in the closed environment, where the template is securely stored.

2 Match On Card

Match On Card has its name from the implementation in smart cards. The match on card technology doesn't exclusively have to be realized with smart cards as the secure device representing the closed environment. The same technology could

also be used together with other secure devices, such as memory cards etc.

This document, however, is focused on the solution where the secure device is a smart card. The document also focuses on fingerprint verification, which is the kind of biometrics most commonly used. The ideal solution for secure biometric verification would be that the fingerprint scanning and the matching were done in the same component. Today, no such device exists.

Another ideal solution would be to send the original fingerprint image directly to the secure device, and that all processing was done there.

As the pre-processing is far too time consuming for today's smart cards, all operations cannot be done entirely inside this closed environment. The security can still be kept by dividing the process into pre-processing and matching and let the matching, where the stored template is needed, be done in the secure device.

The most important thing is that the stored template must never be exposed. Therefore only the part of the verification that requires the stored template has to be done inside the closed environment.

The process can then be described using the following steps (Se Figure 3):

1. The fingerprint image is read from the sensor
2. The fingerprint image is sent into the pre-processing unit. This pre-processing unit could be a PC or another device with enough capacity.
3. The fingerprint is pre-processed and the fingerprint data corresponding to the stored template is extracted.
4. The extracted fingerprint data is sent to the secure device (smart card).
5. The secure device matches the extracted fingerprint data against the stored template.

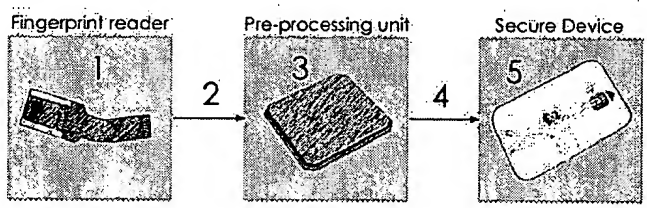


Figure 3: Match on card process.

3 PKI

PKI[1] provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the four principal security functions for commercial transactions:

- Confidentiality - to keep information private
- Integrity - to prove that information has not been manipulated
- Authentication - to prove the identity of an individual or application
- Non-repudiation - to ensure that information cannot be disowned.

3.1 PKI - How does it work?

The principle of PKI is built on the key pair. When a new key pair is generated, it will result in one public and one private key. Both keys are needed to encrypt and decrypt a message. If the message is encrypted with the public key, the private key is used to decrypt, and vice versa. Figure 4 shows how (1) the message is encrypted using the receivers public key. (2) The message is sent encrypted over the net. The receiver decrypts the message (3) using his private key.

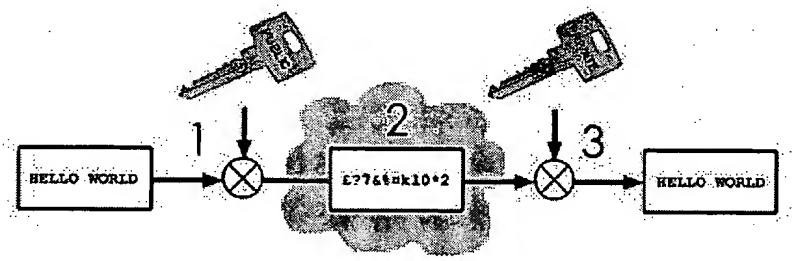


Figure 4: Encryption and decryption using a key pair.

Normally the entire message is not encrypted using the key pair (asymmetric encryption), as it would be a very time consuming operation. Instead a symmetric key is generated for each session and sent to the receiver using his public key.

When creating digital signatures the private key belonging to the sender is used for encryption. The signature can then be verified by the public key of the sender.

In Figure 5 this signature procedure is described. The information that is to be signed passes a known hash function (1) which compresses the data to a fixed

[1]Public Key Infrastructure

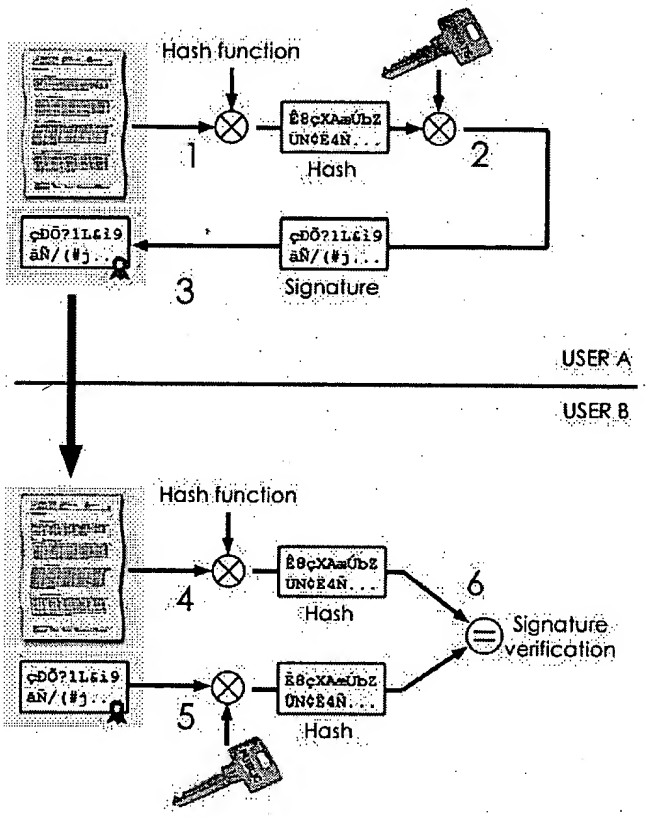


Figure 5: Creating and receiving a signed document, using a key pair.

size. The hash can not be used to reproduce the original document. The hash is encrypted (2) using the private key of the sender (User A). The result of this encryption is the signature, which is placed together with the information in the message (3).

When the receiver (User B) wants to verify the signature, the message is hashed using the same hash function as the sender used (4). The signature is decrypted using the public key of the sender (5). The decryption of the signature using the public key of the sender should then result in the same data as the original hash. If the hash and the decrypted signature matches (6) The signature is considered to be valid.

3.2 The Public Key Infrastructure

A digital certificate contains digital information about the user, such as name, company, e-mail address etc. To create trust we need someone to guarantee the validity of the certificates. Therefore all digital certificates are signed by the Certification Authority (CA). The issuer of the certificates, the Registration Authority (RA), can sometimes be the same instance as the CA, but in large infrastructures they are usually different instances. A comparison can easily be made with the physical world, such as issuing passports, ID cards etc.

Besides being the issuer of digital certificates the CA is responsible for the revocation of expired or stolen certificates. The CA also establishes registers of public keys for the certificates issued.

3.3 The Private Key

As the private key represent the identity of a person it is very important that the key is stored in a secure way. Today the smart card is considered to be the best choice for secure storage of confidential information. As the encryption using the private key is performed by the crypto processor on the smart card itself, the private key is never exposed outside the smart card. Some cards today have also the possibility of generating the keys onboard the chip, which means that the private key is never visible.

However, the cards must be protected in a way that a stolen or borrowed card cannot be used by anyone else but the card holder. The traditional way of protecting smart cards is by using a PIN. Still a PIN can be hard to remember, and they are sometimes written down. The PIN also has the disadvantage as it can be borrowed.

The solution to the authentication problem is using biometrics, which cannot be borrowed or stolen. By using biometrics, we will achieve person to person communication instead of PIN to PIN communication, even in the digital world.

4 Biometrics, PKI and Smart Cards

The only way of securing a smart card with biometrics is to let the match take place in the smart card itself, where the biometric template is stored. If the match is performed outside the smart card there has to be some message sent to the card to unlock it. That message has to be created outside the card, and then the biometrics really doesn't add any security.

With Match On Card technology the smart card can be protected securely with biometrics. The match takes place in the secure environment of the card, where also the template is stored. The card will refuse to admit usage, if the biometrics does not match.

With Match On Card, biometrics will play an important role of making digital certificates personal. The following conclusion can be made.

- PKI ensures security and trust in transactions, where the private key is the weakest point.
- Smart Cards take care of the storage of the private key, where authentication to the smart card is the weakest point.
- Biometrics ensures secure authentication to the smart card.

5 Conclusion

Match On card is a technology to make the biometric matching inside a secure device where the biometric templates is stored. The biometric template will then never be exposed outside the secure environment.

Together with PKI and smart cards, biometrics plays an important role in making the digital certificates personal, by refusing access to the private key without biometric authentication.

References

[1] www.rsa.com

[2] www.baltimore.com

[3] www.verisign.com

[4] www.precisebiometrics.com

For Additional Information

www.precisebiometrics.com

Sweden, Lund

Precise Biometrics AB
Dag Hammarskjlds v.2
SE 224 64 Lund
Sweden

Tel: +46 46 311 100
Fax: +46 46 311 101
E-mail: info@precisebiometrics.com

Sweden, Stockholm

Precise Biometrics AB
Box 1223
SE 164 28 Kista
Sweden

Tel: +46 8 514 426 55
Fax: +46 8 514 426 56
E-mail: info@precisebiometrics.com

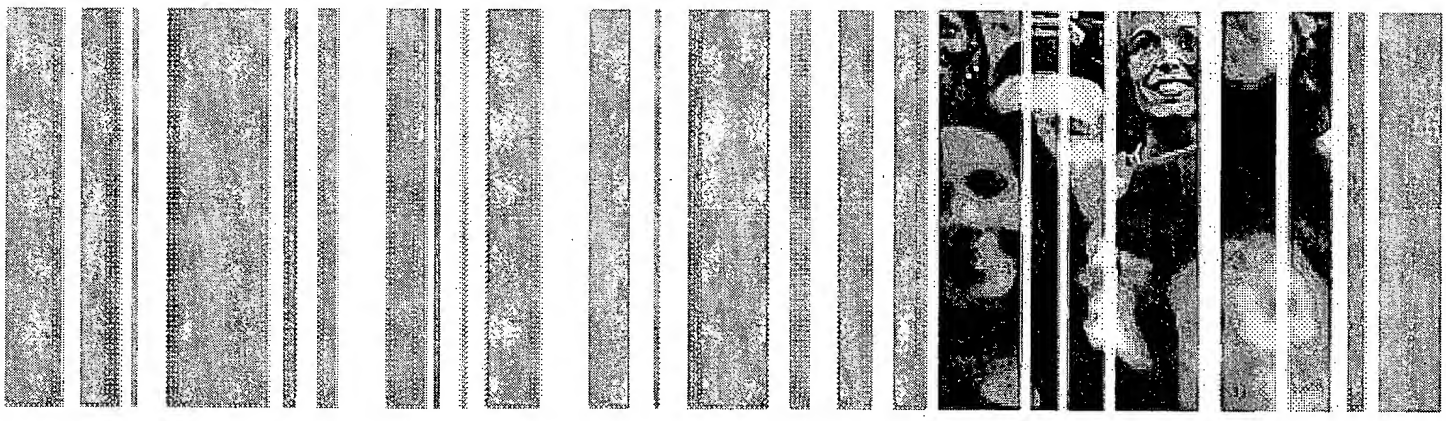
USA, Washington

Precise Biometrics Inc.
8300 Boone Boulevard, Suite 500
Vienna, VA 22182
USA

Tel: +1 703 848-9266
Fax: +1 703 832-0577
E-mail: infous@precisebiometrics.com

[Biometrics and Cryptography]

[Match On Card Paves the Way to Convenient Security]



White paper

utimaco®
safeware

Table of Contents

1 Preliminary Notes

1.1 Abstract

Biometric techniques have now been available for some time. Using these techniques brings a range of benefits, the chief one being that, with them, there is no longer any need to remember a large number of PINs and passwords. This white paper introduces the concepts necessary for understanding the relationships between biometry and cryptographic applications, and the differences between the systems offered by individual suppliers. It also provides details of how biometric techniques are used for PKI-based systems, with the Utimaco product line as an example.

1.2 Document Information

Version: 1.00.03 final, last changed: 16.07.2001.

Author: Richard Aufreiter, Product Manager.

2 Introduction: Passwords, Signatures and Biometry

2.1 Biometric Techniques

2.1.1 Overview

Nature has provided humans with many unique biological (biometric) characteristics that allow us to easily recognise each other in everyday life. When the biometric characteristics of users are used in computer technology, complex algorithms are needed to recognise and match them. However, the benefits are worth the effort since using biometric identification systems for access control will relieve us from having to remember an increasing number of complex passwords, and improve authentication security.

In recent years, many companies have worked to make it possible for computers to identify humans by one of their unique characteristics. There are two kinds of characteristics: active and passive. Passive characteristics can simply be measured, e.g.:

- Face
- Fingerprint
- Iris pattern or retina pattern
- Hand geometry
- DNA etc.

Active characteristics occur when the person has to perform a particular task, e.g.:

- Voice
- Hand-written signature
- Typing behaviour etc.

The question "which is the best biometric method?" cannot easily be answered as it depends heavily on the application involved. All methods differ in cost (mainly for the sensor required), user convenience, accuracy, speed etc. Although DNA analysis might in principle be very accurate, it cannot distinguish between identical twins, and its high cost and low user convenience make it unsuitable for day-to-day business such as PC access. Would you want to give blood every time you logged on to a Windows application? Voice recognition systems on the other hand are low cost, since they simply use a standard microphone as a sensor. However, they can easily be overcome by a tape-recorded voice. The same is true for face recognition.

The most suitable system for IT security is fingerprint recognition. The sensors used for it are now more cost-effective, foolproof and require a low-complexity matching algorithm.

2.1.2 How Does Biometric Recognition Work?

The principle of biometric recognition is the same for all biometric methods. During a process called "enrolment" the system measures one of a user's particular biometric characteristics. From the measurement it generates a "template", which is usually only few hundred bytes in size, and stores it together with the user's name (ID) in (protected) memory on a PC or a smartcard. Usually it is not possible to re-create the original measurement data from this template, but this is also not needed.

During authentication, the user's biometric characteristic is measured again. The template is generated from the current measurement and compared against the previously-stored (enrolled) template. If they are similar enough, it is assumed that the user with the ID stored at enrolment is present.

2.2 Digital Signatures and Certificate-based Authentication

2.2.1 How Do You Create a Digital Signature?

In the age of electronic data processing, digital signatures are playing an increasingly important role. The digital signature should clearly show the intentions of the signing person, for electronic data, just like a signature does on a paper document.

Digital signatures can be used in many ways. With them you can differentiate between trustworthy programs and others, ensure that an e-mail you have received is genuine, and make secure electronic transactions with, for example, banks over the Internet. You can also use the same functions for what is known as "strong authentication" (and also often as "certificate-based authentication").

Digital signatures are created using a secret key (usually RSA) and then checked using a suitable public key. The problem here is that, although normal people can provide a conventional signature, they are not able to carry out encryption with a secret RSA key. They require a computer or similar device that performs this operation on their behalf.

Strictly speaking, a digital signature therefore proves that a document was signed with a particular key, but not necessarily by a particular person. In the case of certificate-based authentication, it is for example assumed that the current owner of a particular secret key is also the user whose unique ID is saved in the certificate that belongs to this key. Consequently it is important that a person protects the secret key assigned to them and do not pass it on to other people, and that they do not obtain it illicitly.

Currently there are two main technologies for "carrying" secret keys:

1. Smartcards

Smartcards are predestined for providing digital signatures. They can be compared with small computers. Smartcards can store data and keys and also execute encryption and signature operations themselves. You can store a key on a smartcard in such a way that it can never read by another device, but instead is only used by the smartcard itself. The data on a smartcard is well protected against unauthorised access from outside, such as electronic measurements or analysis using electron microscopes. Smartcards are easy for the user to move around and can always be close to them.

Using their built-in "computer", smartcards can identify their authorised owner even without the help of other devices. They usually do so by checking a PIN or a password that the user must enter. If the PIN proves correct, the card will create digital signatures for its user. Once the PIN has been saved, it can never again be extracted from the card, and is only used internally by the card itself. The same applies to secret keys.

2. Key files

A cost-effective alternative to smartcards are key files. They usually use a standardised format (PKCS#12). Key files contain one or more secret RSA keys and certificates for a user. The file is encrypted using a PIN or password. Before a user can use the secret key for a signature, they must enter the correct PIN. Although key files are a cheap solution, they do however have a range of disadvantages when it comes to security. As a result, they are only really suitable for providing "unimportant" digital signatures.

In contrast to smartcards, key files can be copied, so the fact that they have been stolen may not even be noticed. You can find out the PIN by trying lots of different combinations. If you tried that on a smartcard, it would lock access after a few attempts. When a signature is being created, the key must be loaded into the computer's RAM in plain text, but on smartcards it always stays on the card.

To summarise, we can see the following:

- Digital signatures are created by computers, using secret keys, and not by people.
- Usually, the authorised owner of a key identifies themselves using a PIN, which causes the computer or smartcard to create a digital signature for them.
- Just because one single person knows a PIN does not necessarily mean that their identity is confirmed. For example, a manager might give their smartcard to a colleague together with their PIN. That colleague can then create digital signatures using their boss's name, and that key.

2.2.2 Can I Sign With My Fingerprint?

In the age of biometry it is naturally tempting to use it for generating digital signatures since biometric features uniquely identify a single person "relatively" well. Unfortunately this is not possible, directly. Inevitably, if you measure the same biometric feature more than once, each measurement differs slightly from the next. An algorithm of varying complexity is used to compare the current measurement result with a previously-saved value (template). If they match closely enough, the current user is accepted as the same person as provided the template.

On the other hand, digital signatures (keys) and passwords for accessing conventional systems require unchanging values that a biometric measurement procedure cannot provide. For this reason a fingerprint or other biometric feature cannot be used directly for a digital signature: it must be provided by one of the "signature devices" (key file or smartcard) described above. However the authorised owner can use biometry to identify themselves to the device, improving the link between the user and the key.

2.3 Ways to Link Signature Devices and Biometry

2.3.1 The Conventional Method: A Password Database

This is certainly the simplest, and also most universal, way to integrate biometry with digital signatures:

1. The user identifies themselves to a target system (usually a PC application) using their biometric feature.
2. The application compares the measured value with the user's reference value (template), which is saved in a database.
3. If the two values match each other sufficiently, the system loads a PIN, which has been saved for the template, from the database.
4. The PIN is then used for a conventional logon at the user's signature device (smartcard or key file).
5. The signature device creates the requested digital signatures.

The user may think that, during this process, they have used biometry (for example their fingerprint) to logon to their signature device, but in fact they did so indirectly using a PIN. This has a range of benefits and disadvantages:

Benefits:

- The user does not have to remember a PIN for their signature device and consequently the PIN cannot get forgotten. This is a general benefit of using biometry for logon.
- The signature device itself does not need to be modified to suit biometry. Conventional devices which may already be in use, such as smartcards, can continue to be used without modification. The biometric logon is set up "by the back door".

Disadvantages:

- The user still enters a PIN to authenticate themselves to the signature device. If someone knows the PIN and is in possession of the device, they can continue to create signatures without undergoing biometric recognition beforehand.
- If the user knows the PIN, they can still hand over the signature device to other people, who can then create signatures with it. It is not possible to uniquely assign a signature to a user.
- Major disadvantage: the PIN for this signature device (and the PINs for all other users of the system) is stored in a database and not only in the user's memory. If an attacker hacks the database, to obtain its data, or listens in to the communication between the database and the client PC, they can obtain the PIN and use it to log themselves on to the user's signature device.
- If an attacker succeeds in replacing an authorised user's template in the database with their own, the attacker can logon to the system and the system will log them on to the user's signature device (which may previously have been stolen).

2.3.2 Match On Card: Logon with Fingerprint

Smartcards are currently the best technical solution, in terms of security, for generating digital signatures. As they are even able to carry out computing operations independently, smartcards can also be enabled for carrying out biometric techniques. The idea on which the "Match On Card" procedure is based is amazingly simple:

Instead of a PIN, an non-downloadable biometric template for the authorised user is stored on the card. To authenticate themselves to their card, and activate the signature functions, the user does not send a PIN to the card, but instead a current scan of their biometric feature. Instead of comparing a PIN character by character, the card compares the current scan with the saved template using a biometric comparison algorithm (which is why the name "Match On Card" is used). Despite the fact that the comparison algorithm is more complex, the underlying process is almost identical to logon using a PIN. Currently the fingerprint is used as a biometric feature in such systems.

The first technology demos of this principle were presented at the CeBIT 2000 trade fair. Smartcards with this functionality have been commercially available since the end of the year 2000. The first real IT security applications based on this technology were presented at CeBIT 2001 by the German company Utimaco Safeware AG. The SafeGuard® Biometrics product not only extends the Utimaco Safeware file encryption, authentication, VPN and digital signature product portfolio by adding the option of using with Match On Card. It also offers special drivers, consisting of PKCS#11 and CSP modules, with which standard applications such as Netscape or Microsoft Internet Explorer, Outlook etc. can also use biometric smartcards of this kind.

In terms of the currently-available technology, Match On Card is the best way to integrate biometry and cryptography. However, it also presents its own benefits and disadvantages:

Benefits:

- Genuine direct logon using the biometric feature (fingerprint). PINs are not used any more, so they cannot be forgotten or given to someone else.
- The biometric feature is stored and checked directly in the card so there is no more need to manage a separate database for storing templates or PINs. This means many potential methods of attack are no longer available. This also simplifies the installation and administration of software, since there is no longer a need to install or replicate databases of this kind.
- User mobility is supported. All the data needed to verify a user's biometric feature is stored on their card, so the user can also work off-line, without a connection to a template server, and still create digital signatures.
- No more worries about data protection. Many users feel unhappy to know that their biometric data is stored in a central database. With Match On Card, these worries disappear since the user always hold this data on their card, which is with them, and the data cannot be obtained from the card in any way, not even once.
- High levels of compatibility with existing IT security solutions. The only thing that changes is the method for logging on to the smartcard. However, the cryptographic process is still identical to the one used in a "normal" smartcard solution, so Match On Card systems provide an ideal way to upgrade existing IT security applications. Using suitable PKCS#11/CSP drivers such as the ones supplied by Utimaco Safeware, even some applications that are actually not directly capable of using biometry (e.g. MS Internet Explorer, MS Outlook or Netscape) can use smartcards of this kind for cryptographic services.

Disadvantages:

- Cannot be used for solutions based only on software, with key files instead of smartcards.
- Although a "biometric" data stream is sent to the card, instead of a PIN, and the comparison algorithm is more complex, it is nevertheless still only a data stream and so it can be seen as just a very long PIN. Ideally the sensor and signature unit form one integrated device.
- Match On Card cannot be used with all smartcards. To set up a Match On Card system, the biometry system supplier needs to work with the smartcard manufacturer. However implementation details can be hidden from the application by using suitable PKCS#11 or CSP drivers.

Not all biometric techniques are suitable for Match On Card. Smartcards have only very restricted computing power compared with current Pentium PCs. It is essential for the biometric processes to be processed in the smartcard in a reasonable amount of time, e.g. one second, despite its poor processing capabilities. In addition, the biometric templates must not take up too much memory as that is also restricted on smartcards. Fingerprint procedures have proven the most suitable for Match On Card.

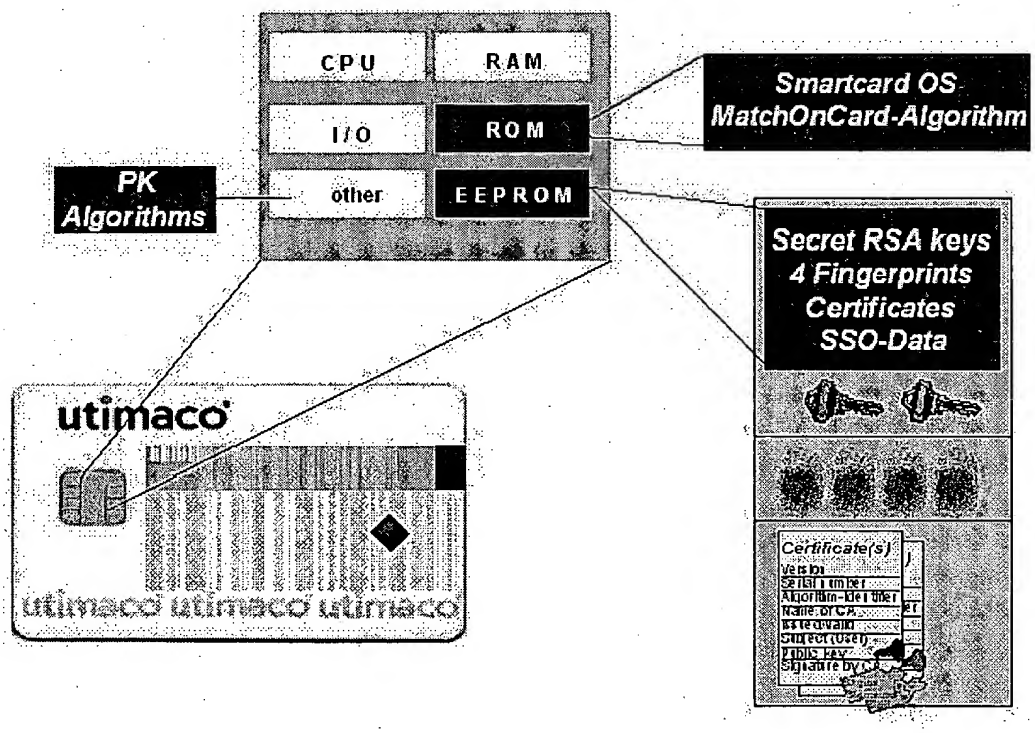


Figure 1: The Biometric Smartcard

The figure shows a schematic overview of smartcards, which have a similar structure to small computers, and their logical components. These include the operating system, keys, certificates and biometric templates.

You should not confuse Match On Card solutions with others that, on first glance, appear similar because they use biometry and smartcards, but are not as convenient, and offer less security. Before Match On Card technology appeared, and maybe even today, some manufacturers often created biometric templates on conventional smartcards. However, these were then read from the card during logon and compared in the PC's RAM. Unfortunately, this procedure does not unlock the card, which is still protected by the PIN. This means that the PIN either has to be loaded from a database (which compromises security) or that users must enter yet another PIN as well as their biometric features (which is inconvenient).

2.3.3 Signature Devices with Full Biometric Capability

In theory, the best possible solution for combining biometry and digital signatures is obviously devices which bring together the signature function, key memory and biometric sensor (including the verification algorithm) in one single case which is protected against interference. This device would then be able to tell whether the biometric features it receives are genuine and up-to-date and to make the signatures it creates dependent on them. If this device were to integrate all these functions in a tamper-proof case, the only way to access a signature illegally would be to forge the biometric feature of the legal owner. Fortunately the improved recognition functions in many current sensors mean that this is becoming more and more difficult.

The ideal model for this type of device would be, for example, a smartcard with an integrated fingerprint sensor. These devices are currently being developed by various manufacturers. However the technology is not yet so advanced that these devices can be produced cost-effectively for use in everyday situations with the required levels of security. Therefore, for the foreseeable future, Match On Card will enable the best-possible combination of biometry and cryptography.

2.4 Practical Examples of How to Use Biometry-enabled Smartcards

2.4.1 Personalising the Card – From the PKI to the User

If you want to implement smartcards with the technology currently used by Match On Card, you are faced with a few practical questions, such as "What is the life cycle of this type of smartcard?" How can I store the key, certificates and biometric data on the card? How can I make sure that the biometric data is genuine?

The first major point is that you can keep the generation of keys and certificates quite separate from the card's biometric functions. As a result the process shown below is completely independent of the PKI that is being used. Both the examples shown below illustrate how the life cycle of a smartcard with Match On Card capability may start in real life. In the examples, the smartcard has been personalised centrally by a "Registration Authority" (RA), because this will be the most common scenario where security is a critical issue. Other methods of card personalization are based on a similar principle.

Example 1: central enrolment – optimum authenticity of biometric information:

1. The customer (the PKI operator) buys white (blank) or printed cards from the smartcard manufacturer.
2. The cards are sent to the RA stations of the customer's PKI.
3. The RA stations personalise the cards in the usual way (with PINs, certificates, keys, or other data if required) and PIN letters.
4. The cards are returned to the user, but the PIN letters are sent to the "enrolment station" (this may also be the RA). The "enrolment station" is an application which is used to register fingerprints for the first time on the card for later use in a Match On Card. Before this takes place, the card (like any other card) can only be used with a PIN.
5. When the user receives their card, they are still not able to use it because they do not have the PIN letter. Therefore they must take their card to the enrolment station. (This is not necessary if the RA and enrolment station are the same device if the user is present when their card is personalised.) The user registers their fingerprint under the supervision of the Enrolment Officer after the card is given the PIN from the PIN letter. This ensures that only the fingerprint of a legal user is registered!
7. When the registration is successful, the card's PIN can be deactivated (if required). After this the card can only be used by presenting a registered finger. The user can now use the card for signatures and other tasks. If, for physical or other reasons, a user is unable to register their fingerprints, they can still use the card with its PIN.
8. This procedure can be used in the same way even without PKI, if chipcards with biometry but without a signature function are to be used.

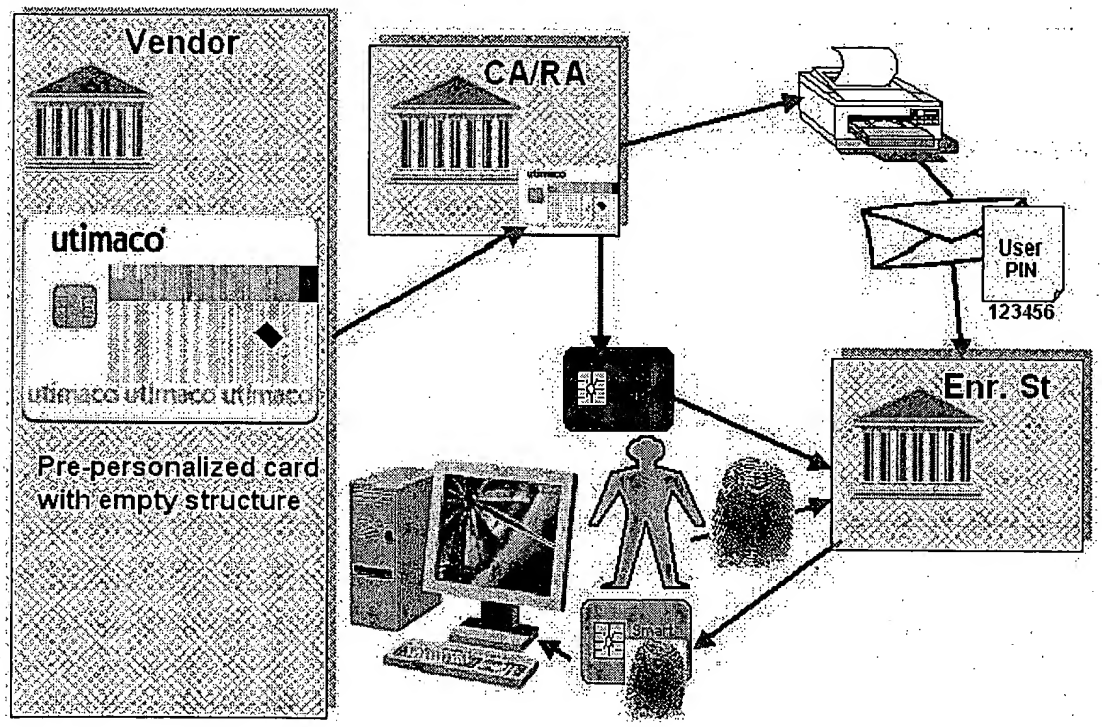


Figure 2: Central Enrolment

Example 2: local enrolment – optimum user-friendliness:

1. The customer (the PKI operator) buys white (blank) or printed cards from the smartcard manufacturer.
2. The cards are sent to the RA stations of the customer's PKI.
3. The RA stations personalise the cards in the usual way (with PINs, certificates, keys, or other data if required) and PIN letters.
4. The cards are returned to the user with the PIN letter.
5. When the user receives their card, they insert it into their card reader for the first logon. If the software is correctly set up, it recognises that this is a card with biometric capability and requests the user to register their fingerprint after the user has identified themselves by entering the PIN from the PIN letter.
7. When the registration is successful, the card's PIN can be deactivated, if required. The user can now use the card for signatures and other tasks. If, for physical reasons, the user is unable to register their fingerprints, they can still use the card with the PIN.
8. In this scenario no organisational overheads are required for biometry in comparison with a conventional smartcard solution. However, the user must be trusted to only register their own fingerprints.

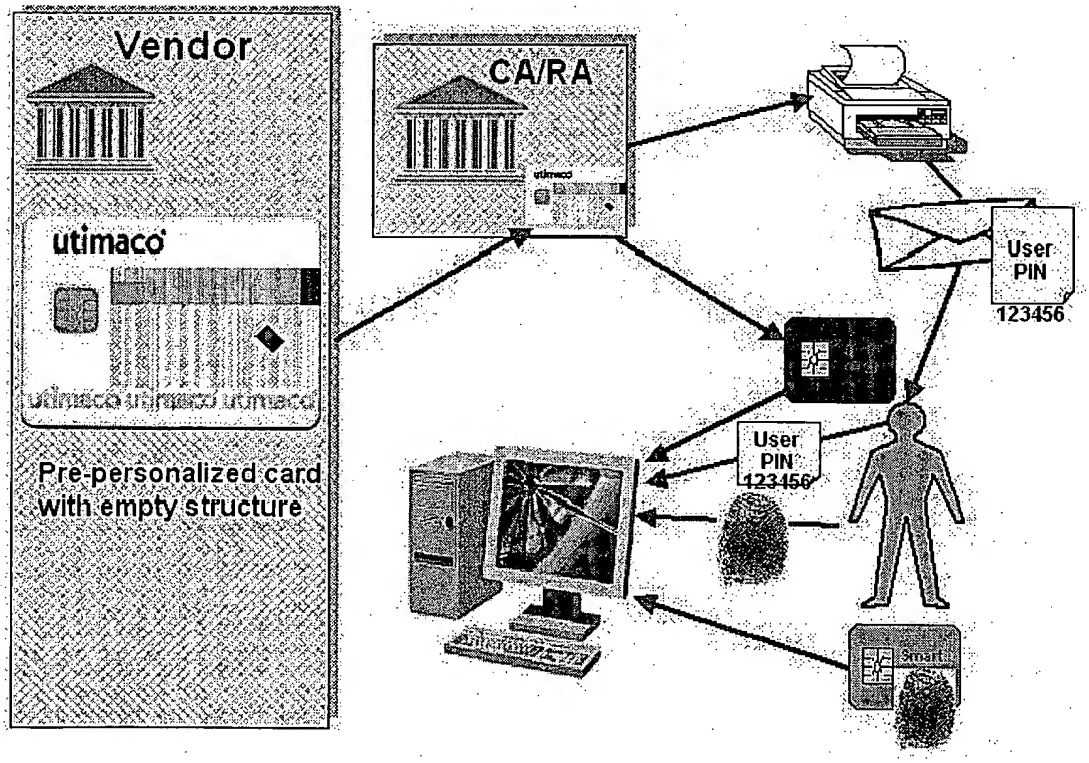


Figure 3: Local Enrolment

Of course, depending on the intended use and technology, slightly different procedures may be used as alternatives to the Match On Card examples described above. Nevertheless it is important that:

- Certificates actually only involve keys and unique user IDs, and have nothing to do with the technical aspects of biometry and that

- the initial registration (the "enrolment") of biometric features that are used to create the logical assignment between the keys and features takes place under correct supervision. This is because at this point in time the signature device itself is still unable to distinguish between authorised and unauthorised users.

2.4.2 Digital Signature with Fingerprint and Smartcard

In everyday life biometry-enabled cards are used in a very similar way to normal smartcards. If the user has the appropriate software, usually installed as a plug-in in a mail system or an Office application, the program will request them to place their finger on the sensor when their signature is required. Either the user will decide what is to be signed by selecting the appropriate option, or this will be pre-defined by their administrator.

If the card recognises the fingerprint correctly, the card will meet the application's request to create a signature and will therefore sign the data (usually an e-mail or a document). As in non-biometric systems, only the user's public certificate is required to verify the validity of a signature. No smartcard is required for this.

Therefore the only (but crucial) visible difference for the user is the fact that they simply need to place their finger on the sensor instead of entering a password. The rest of the procedure remains identical to "normal" signature applications.

Examples of currently-available applications which provide this feature are SafeGuard® Sign&Crypt from Utimaco Safeware, as PKCS#11 and CSP plug-ins for its product SafeGuard® Biometrics.

2.5 Passwords and Biometry

2.5.1 Single Sign On Systems

One of the main reasons for implementing biometric recognition is to relieve users of having to remember dozens of passwords. The systems should be able to recognise their authorised users.

However, most current IT applications are not able to handle biometric data. They must be specially modified to do so. Similarly, most applications must also be specially modified so that they can handle encryption. Despite this, there are already a number of Single Sign On (SSO) applications available that can help reduce the number of passwords. These applications store user passwords in an encrypted database or on a smartcard. When the user has identified themselves to the database (usually once again by means of a password), the SSO applications transfer the passwords (without any additional user involvement) into the password-based login dialogues of other existing applications.

These applications are offered by a wide variety of manufacturers with, in some cases, huge differences in functionality, user-friendliness and security. The advantage of implementing this type of system is that most applications do not have to be modified in order to use SSO. Usually Single Sign On Systems still have nothing to do with biometry. They still use passwords to identify their users in the traditional way.

2.5.2 Can Biometry Replace Passwords?

As already shown in section 2.2.2 "Can I Sign With My Fingerprint?, even today it is still not possible to generate a constant value (such as a key or a password) directly from the measurements of a biometric feature. As a result, there are two methods of using biometry as a replacement for a password:

1. The device / system knows how to use biometric data and carries out a biometric comparison instead of the usual password comparison. This category includes all smartcards with Match On Card capability for which a fingerprint can be used to replace a PIN. See also 2.3.2 "Match On Card: Logon with Fingerprint".
2. The biometric feature is compared with previously-stored reference values (templates) in a database and the actual password, which was saved along with the template, is then fetched from this database See also 2.3.12.3.1 "The Conventional Method: A Password Database".

Both the examples shown above illustrate how logon to a SSO system can be implemented with biometric data. After this, the user uses passwords in the conventional way to access conventional applications.

2.6 Practical Examples of Biometric Logon

2.6.1 Biometric Logon with a Database

There are as many programs that users use to biometrically logon to operating systems as there are stars in the sky. Almost every manufacturer of biometric recognition devices offers this type of application for their device, solely in order to demonstrate their device's functionality. Depending on the manufacturer, they may also offer functions such as Single Sign On for other applications as well as the option of storing encrypted files on a "virtual" hard disk drive.

All these applications operate on the basis of the template/ password database principle described above. Once the user has registered their features and passwords, they can logon by simply presenting their biometric feature instead of having to enter a password.

These applications vary enormously when it comes to security and usability in large-scale environments, for example if many users need to use a large number of machines in different locations. Because of their shared underlying principle, these applications have the following things in common:

- The application can be very cost-effective because it is a pure software solution. If the voice or face is used as the biometric feature, standard commercially-available web cams or built-in microphones can be used as the biometric hardware.
- Obviously, security is reduced if the user is not required to enter a password in addition to their biometric feature. However, because it is not possible to derive a key directly from the features, the useable data in the password database can only be protected in a basic way by, for example, a constant key.

- If you want to use biometry for long-term IT security, there is one main feature to look for when selecting the application: can it be extended for bigger user groups and cryptographic applications? Many of the applications supplied with biometric devices by biometrics manufacturers offer a specifically-defined range of functions, and cannot be upgraded to use digital signatures or similar functions. For a serious implementation, you must first select a suitable application and only then decide which particular biometric procedure you will use. In this case, Match On Card applications have a clear advantage.

2.6.2 Biometric Logon with Match On Card Smartcard

Just as described in the chapter about digital signatures, smartcards with Match On Card capability are also especially suitable for biometric Single Sign On. In this case the data is stored in the protected area of the card with the format "application name, user ID, password". This card only makes this data accessible after its owner has identified themselves. In the situation we are interested in, this naturally takes place when the card uses Match On Card to compare a biometric feature instead of a PIN.

After the user has successfully identified themselves to the card the SSO application can read the entries from the card and transfer the passwords to other applications for logon if required. The same cards can, of course, also be used for digital signatures or similar procedures.

The advantage of these methods is the clear improvement in security compared to a pure software solution, as well as less complex administration, especially for mobile users. The user has all the data that they require with them on their card.

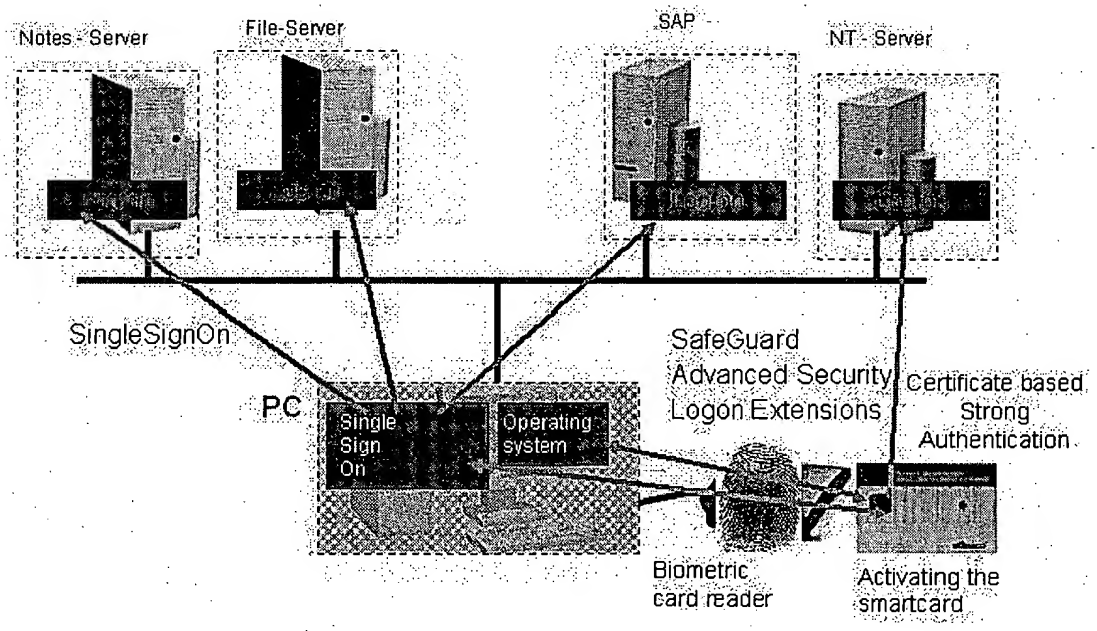


Figure 4: Single Sign On via Smartcards

Applications like SafeGuard® Advanced Security from Utimaco Safeware, for example, offers this type of solution together with many further options for securing data in an IT system.

2.7 Looking to the Future

Even today, biometric applications are still a rare species in the PC environment. However, due to the falling prices for biometric sensors, new Match On Card technology, and improved interoperability between the manufacturers, they will become more widespread in the near future and will replace password systems in the medium term.

In the longer term, the fusion of mobile phones, small computers (PDAs) and smartcards will mean that most people will have a personal digital assistant which connects them with the "electronic world" and, activated by biometry, will also provide digital signatures. The right passport to the digital world.

3 SafeGuard® Biometrics

3.1 Preface

In modern IT environments, data security is becoming an increasingly important issue. Complex cryptographic protocols are frequently used, but their keys are often inadequately protected. Even the relatively high security offered by smartcards cannot improve this because key data can only be accessed by users who know the correct PIN.

In comparison with a PIN, biometric recognition of a user can achieve a much closer link between the user and their smartcard. As a result, because a PIN is no longer required for identification it cannot be lost, forgotten, given to someone else or stolen.

3.2 What is SafeGuard® Biometrics?

3.2.1 Biometric Support for IT Security Applications

With SafeGuard® Biometrics, biometric authentication procedures can be integrated into IT security applications. The current version has the unique ability to make smartcards with Match On Card capability available for use by a wide spectrum of applications. These smartcards are able to identify their correct user by means of a biometric feature (fingerprint) instead of a PIN.

The standard configuration of SafeGuard® Biometrics consists of two main components:

1. The biometric base module

The biometric base module provides a range of drivers which allow other applications to use smartcards with Match On Card capability and therefore to authenticate users by biometry instead of a PIN. The special design of these drivers means that the application itself no longer needs to be modified to use biometry. SafeGuard ® Biometrics takes care of the details. In particular, the base module provides the following applications with biometric capability:

- **Netscape Communicator, Messenger** and other PKCS#11-based applications. PKCS#11 Provider from SafeGuard® Biometrics has a range of biometric functions which allow these applications to use Match On Card smartcards in the same way as conventional smartcards. If the logon function is called up without a PIN, the module carries out the biometric authentication itself. This makes it possible, for example, to create signed or encrypted e-mails, as well as certificate-based SSL authentication. Any of the PKI systems supported by Netscape can be used.

- **Microsoft's Internet Explorer, Outlook, Outlook Express, Office** and other Crypto API (CSP)-based applications. With SafeGuard® Biometrics' biometrically enabled Cryptographic Service Provider (CSP), these applications can use Match On Card smartcards in the same way as conventional smartcards. As a result, for example, signed or encrypted e-mails can be created as well as certificate-based SSL authentication and the signature of Office macros. Any of the PKI systems supported by these applications can be used.
- **SafeGuard LANCrypt, Sign&Crypt, Advanced Security, VPN** and other CryptWare Toolkit or CardMan API-based products. With the biometric drivers supplied by SafeGuard® Biometrics, these applications can use Match On Card smartcards in the same way as conventional smartcards. This provides access to a wide range of professional security functions, used together with biometry, that cannot be provided by standard applications on their own. They include transparent file encryption for secure data storage, smartcard-based Single Sign On, certificate-based authentication, even for NT systems without Kerberos, signed and encrypted e-mails and documents etc. Any of the PKI systems supported by these applications can be used.

The entry-level equipment also includes the optional "enrolment station" which is used for the initial registration of fingerprints on a formerly PIN-protected smartcard that has biometric capability. This allows you to create and distribute cards even with PKIs that have not been specifically modified for biometry.

2. Windows logon including desktop monitoring (GINA)

With these optional components, users can logon to the Windows operating system by using a biometrically-activated smartcard. This means the logon password is no longer needed. If the smartcard is removed, the Windows desktop is automatically blocked. This basic functionality can be extended by adding other SafeGuard products later, to match customer requirements.

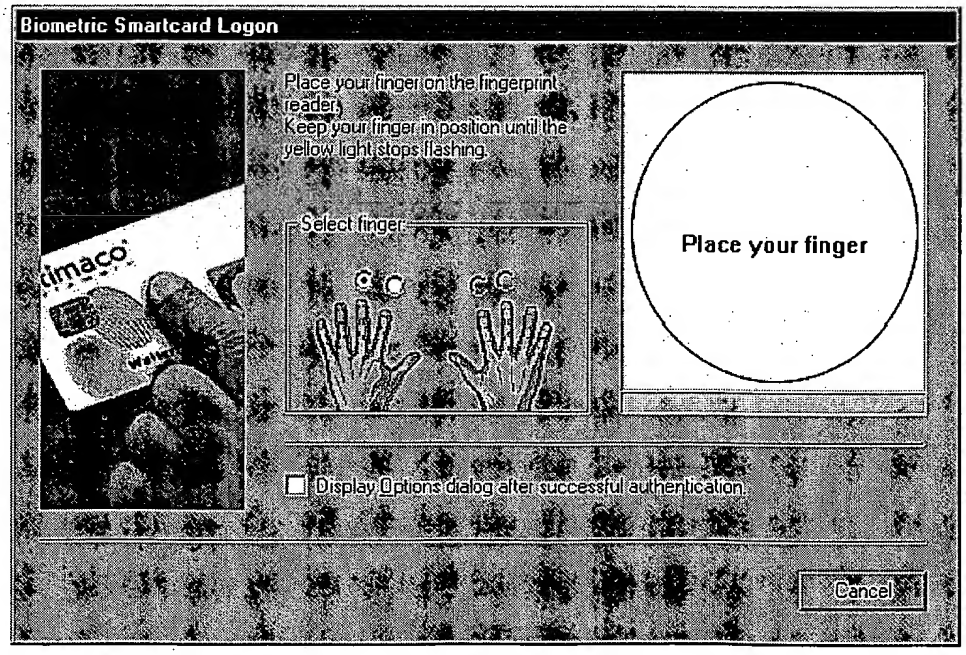


Figure 5: Biometric Logon Dialog

3.2.2 Advantages of using SafeGuard® Biometrics

At present, the SafeGuard® Biometrics solution supplied by Utimaco is the only solution on the market which operates with the innovative "Match On Card" technology and therefore can provide significantly higher security, as well as investment protection, because of the future development of its functionality. The most important advantages of SafeGuard® Biometrics:

- **Very user-friendly**: users logon biometrically, using a fingerprint, so they no longer need to remember a smartcard PIN. The integrated Single Sign On module in SafeGuard Biometrics and Advanced Security means that users are freed from the burdens of password-based logons to operating systems and many other applications such as SAP, terminal servers, Lotus Notes etc. The smartcard carries this out completely automatically.

- **Cost savings for the hotline**: biometric logons and the Single Sign On functionality mean that forgotten passwords are a thing of the past. This not only reduces the costs for hotline/system administration in large-scale environments, but also increases productivity because users no longer need to sit around waiting for the administrator to reset their forgotten password.

- **Highest possible levels of security**: the biometric template is not only stored on the smartcard but also compared by the card itself with the current biometric scan. Unlike in conventional biometric systems, the template can never be removed from the card. Neither PINs nor templates are stored in a database (which may be faced by attacks). Since biometry replaces PINs, unauthorised persons cannot cause damage by obtaining PINs illicitly.

- **Simplified administration and user management**: no central template database is required, so roaming users and local user authentication are not a problem. Everything needed for authenticating the user is on their smartcard, which they carry with them. There is no template database that needs to be replicated on different machines or at different locations, or needs to be constantly available.

- **Investment protection**: most other biometric solutions only offer a fixed range of functions, mostly logon to the operating system + SSO, but no cryptographic functions. In contrast, the functionality of SafeGuard® Biometrics can be extended without replacing the hardware. For example, you can add digital signature applications, transparent file encryption, strong certificate-based authentication, quick change of users at a workstation, virtual private networks (VPNs) etc.

- **Support for standard applications**: SafeGuard® Biometrics is supplied with, among other things, drivers that comply with current standards (PKCS#11, CSP), with which smartcards **with biometric logon** can also be used in standard applications such as Netscape, Microsoft Internet Explorer, Microsoft Office or Microsoft Outlook Express. Currently this range of functionality is unique among biometric solutions.

3.2.3 Technical Data Version 1.0

Target platform:

Microsoft Windows NT 4.0 SP6, Windows 2000 SP2 on Intel platforms.

Biometry-enabled smartcards:

Chip type: Atmel AT90SC3232C – 32KB EEPROM
Operating system: MioCOS 1.1

The smartcards are preformatted before delivery, and supplied with default PINs, files for two 1024-bit RSA key pairs, associated X.509 certificates, four fingerprint templates (so that alternatives can be used, if a user injures one of their fingers), Single Sign On and PKCS#11 data fields. Special customer-specific formats available on request.

Alternative:

Atmel AT90SC6464C – 64KB EEPROM
Operating system: MioCOS 2.0
Available from the fourth quarter of 2001

Smartcard Reader Precise 100SC:

Smartcard reader combined with fingerprint sensor. PC/SC-compatible. Two versions are available. Neither of them requires its own power supply unit:

1. With a parallel port for use under Windows NT or Windows 2000. The computer's parallel port must support ECP mode. The reader is usually supplied with power via a PS2 keyboard power-takeoff plug, which is also supplied with it.
2. With USB connection for use under Windows 2000. Again, the power is supplied via the USB connection. The readers are Plug&Play-compatible.

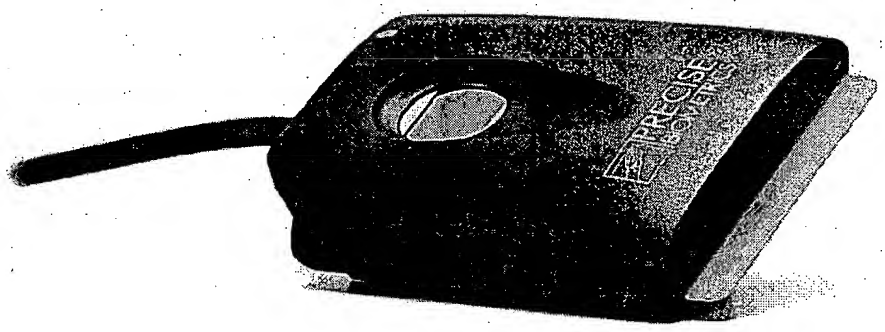


Figure 6: Biometric Smartcard Reader

Other details:

- Alternative logon to smartcards also possible using a PIN, so systems without a biometric card reader can also be used with the same card.
- Mixed operation of smartcards that have different operating systems, with or without biometric capability at runtime, without additional configuration. In this way, for example, it is possible to gradually implement biometric functionality in a system with an existing conventional smartcard infrastructure, without having to equip all users with new cards at once.
- Central administration using Windows policies in the Microsoft Management Console.
- Version 1.0 includes a PKCS#11 module for cards with PIN logon. A PKCS#11 update is available with biometry logon or CSP via CardMan API 3.41 or, in a later version, SafeGuard® Biometrics.

Future versions of SafeGuard® Biometrics will support other types of biometric devices and smartcards.

3.3 Examples of Practical Applications

3.3.1 Digital Signature of E-Mail and Documents

E-mails can be signed digitally and encrypted using the base modules supplied, or using SafeGuard® Sign&Crypt. This permits confidential data exchange over the Internet. The digital signature guarantees that a message has not been falsified on its way to the recipient.

Once the PKI has assigned the smartcard certificates and keys, and the user has registered their fingerprints, the user can use the smartcard. In the user's e-mail program settings the user activates the functions for digital signature and encryption. When the user send the e-mails, they use their fingerprint to report their presence to the smartcard. After, the application uses the smartcard to digitally sign the e-mail.

3.3.2 Single Sign On to Other Applications

Used together with SafeGuard® Advanced Security, SafeGuard® Biometrics can save the user from having to remember a large number of passwords. The user only has to use their finger print once, to logon to the smartcard. The data saved on the smartcard is then used automatically to log the same user onto other applications that are not smartcard-enabled, such as Lotus Notes or terminal clients.

3.3.3 Powerful Certificate-based Strong Authentication

Used together with SafeGuard® Advanced Security or VPN, SafeGuard® Biometrics can use biometric smartcards for authentication with certificates corresponding to the X.509 standard. If the SafeGuard® extensions are installed on a Windows server they ensure that only clients with users who have a valid certificate can logon to the server. This is means that simply knowing a Windows password (which may have been stolen or revealed to someone else) is no longer enough to compromise system security.

3.4 Summary

Through the unique design of SafeGuard® Biometrics, all smartcard-based IT security applications can now also be implemented with biometric logon instead of a PIN. For the first time, its innovative Match On Card technology ensures that no compromises are made in security or ease of administration. With suitable drivers, biometry can even be used in common standard applications such as those from Microsoft or Netscape, as well as allowing problem-free integration of biometry into existing IT infrastructures.

The examples above are just a few of many other implementations that can be achieved with SafeGuard® products.

4 Terminology

4.1 Abbreviations

CA	(**C**ertification **A**uthority): Application which acts as a "trustworthy instance" in PKI systems and signs both user certificates and CRLs. The CA is usually implemented as a service without a graphical user interface. This service is provided for use by the RA that requests certification of keys from the CA.
CIS	**C**ard **I**ssuing **S**ervice
CSP	(**C**ryptographic **S**ervice **P**rovider): Software module in the sense of a driver that allows applications based on the Microsoft CryptoAPI to access cryptographic devices such as smartcards.
GINA	(**G**raphical **I**dentification and **A**uthentication): Interface defined by Microsoft which controls the desktop and login to Windows NT/2000/XP.
MOC	(**M**atch **O**n **C**ard): Technology offered in certain smartcards with which a biometric template comparison is carried out on the card instead of comparing a traditional PIN, to authenticate the user.
PIN	(**P**ersonal **I**dentification **N**umber): Combination of numbers or letters with which a user authenticates (identifies) themselves to a system. The expression "PIN" is often used in connection with smartcards while the expression "password" is usually for software applications.
PKI	(**P**ublic **K**ey **I**nfrastructure): Set of applications that together administer the life cycle of keys in public key systems. The main components of a PKI are a CA and an RA.
RA	(**R**egistration **A**uthority): Application for registering users in public key systems and blocking them from it. Basically the user interface for a CA. The CA and RA do not usually run on the same machine.
SSL	(**S**ecure-**S**ocket-**L**ayer): Standard mechanism integrated in WEB browsers to perform encrypted and/or authenticated communication between a client and a WEB Server.
SSO	(**S**ingle-**S**ign-**O**n): SSO systems provide the user with an environment that automatically logs them onto other systems (after one-time authentication on the SSO system), mostly by passing on passwords.

4.2 Glossary

Enrolment	Synonym for the process of generating a "reference template" of a biometric feature for a person, with which a current measurement can later be compared. For example, the optimal value of three measurements of the same finger print is determined and then stored on a smartcard or in a template database.
Template	Data record, generally a few hundred bytes in size, which contains summarised information about a biometric feature for a person. This template is compared with one that is generated from a current measurement in order to identify a person biometrically. Since two measurements never give exactly the same result, complex algorithms are used to perform the matching. Usually it is not possible and also not necessary to use a template to regenerate the associated set of measurement details for a biometric feature (one-way function).
Smartcard	Also known as a "chip card". Chip that is secure from interference, with its own computing capacity, in which protected data values are stored and signatures can be created. Smartcards are able to recognise their owner by internally checking a password (referred to here as a PIN) or by checking against a biometric template.

5 Additional Information

If you would like to find out more about biometric security products with Match On Card technology, please contact your nearest Utimaco distributor or visit our website:

http:// www.utimaco.com

Utimaco Safeware AG, D-61440 Oberursel, Fed. Republic of Germany